S. HRG. 114–322

INTERNAL REVENUE SERVICE DATA THEFT AFFECTING TAXPAYER INFORMATION

HEARING

BEFORE THE

COMMITTEE ON FINANCE
UNITED STATES SENATE

ONE HUNDRED FOURTEENTH CONGRESS

FIRST SESSION

JUNE 2, 2015

Printed for the use of the Committee on Finance

U.S. GOVERNMENT PUBLISHING OFFICE

20–958—PDF WASHINGTON : 2016

For sale by the Superintendent of Documents, U.S. Government Publishing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON FINANCE

ORRIN G. HATCH, Utah, *Chairman*

CHUCK GRASSLEY, Iowa
MIKE CRAPO, Idaho
PAT ROBERTS, Kansas
MICHAEL B. ENZI, Wyoming
JOHN CORNYN, Texas
JOHN THUNE, South Dakota
RICHARD BURR, North Carolina
JOHNNY ISAKSON, Georgia
ROB PORTMAN, Ohio
PATRICK J. TOOMEY, Pennsylvania
DANIEL COATS, Indiana
DEAN HELLER, Nevada
TIM SCOTT, South Carolina

RON WYDEN, Oregon
CHARLES E. SCHUMER, New York
DEBBIE STABENOW, Michigan
MARIA CANTWELL, Washington
BILL NELSON, Florida
ROBERT MENENDEZ, New Jersey
THOMAS R. CARPER, Delaware
BENJAMIN L. CARDIN, Maryland
SHERROD BROWN, Ohio
MICHAEL F. BENNET, Colorado
ROBERT P. CASEY, Jr., Pennsylvania
MARK R. WARNER, Virginia

CHRIS CAMPBELL, *Staff Director*
JOSHUA SHEINKMAN, *Democratic Staff Director*

CONTENTS

OPENING STATEMENTS

WITNESSES

ALPHABETICAL LISTING AND APPENDIX MATERIAL

INTERNAL REVENUE SERVICE DATA THEFT AFFECTING TAXPAYER INFORMATION

TUESDAY, JUNE 2, 2015

U.S. SENATE,
COMMITTEE ON FINANCE,
Washington, DC.

The hearing was convened, pursuant to notice, at 10 a.m., in room SD–215, Dirksen Senate Office Building, Hon. Orrin G. Hatch (chairman of the committee) presiding.

Present: Senators Grassley, Crapo, Roberts, Enzi, Cornyn, Thune, Isakson, Heller, Scott, Wyden, Stabenow, Nelson, Carper, Cardin, Bennet, and Casey.

Also present: Republican Staff: Chris Campbell, Staff Director; Kimberly Brandt, Chief Healthcare Investigative Counsel; Chris Armstrong, Deputy Chief Oversight Counsel; and Justin Coon; Detailee. Democratic Staff: Adam Carasso, Senior Tax and Economic Advisor; Dave Berick, Chief Investigator; Michael Evans, General Counsel; Daniel Goshorn, Investigative Counsel; and Joshua Sheinkman, Staff Director.

OPENING STATEMENT OF HON. ORRIN G. HATCH, A U.S. SENATOR FROM UTAH, CHAIRMAN, COMMITTEE ON FINANCE

The CHAIRMAN. The committee will come to order.

Our hearing today concerns recent revelations that the Internal Revenue Service was the target of an organized service breach aimed at roughly 200,000 taxpayer accounts. We understand that over 100,000 of these breaches were successful, with cybercriminals obtaining confidential taxpayer information from the agency's Get Transcript application.

In dealing with this breach here in the Senate, this committee stands alone, having legislative jurisdiction over the Internal Revenue Code, oversight jurisdiction over the IRS, and wide-ranging abilities to conduct investigations dealing with individual taxpayer information.

While I have raised questions in the past about the way the IRS prioritizes its spending, today's hearing is about finding out how criminals stole vast amounts of taxpayer information. Any questions regarding funding levels for the agency should wait until we have a complete understanding about what occurred.

Before we turn to the technological issues, let us focus for a moment on the victims. Because of this breach, criminals were able to get personal information about roughly 104,000 taxpayers, potentially including Social Security Numbers, bank account numbers, and other sensitive information. These taxpayers, and their

families, must now begin the long and difficult process of repairing their reputations. And they must do so with the knowledge that the thieves who stole their data will likely try to use it to perpetrate further fraud against them.

Commissioner Koskinen, put simply, your agency has failed these taxpayers.

This hearing is of utmost importance as we work to find out what individuals and organizations were behind this breach; discover how this breach occurred and what steps the IRS might have taken to prevent it; find out what taxpayer information was compromised and how this may affect both taxpayers and tax administration going forward; and determine what tools and resources are necessary to better protect taxpayers, catch cyber-criminals, and prevent this type of breach from being successful in the future. Most of all, we must pledge to work together to make sure that this type of breach does not happen again.

The secure movement of information is the lifeblood of international commerce and a necessary predicate for efficient government administration. Unfortunately, this information is also highly valuable to criminals.

We see it in the headlines nearly every week: a major insurance company, bank, or retailer has its information security compromised, and personal information or corporate data is stolen. Federal departments, especially defense-related agencies, come under attack each and every day.

The IRS is not, and will never be, exempted from this constant threat. In fact, there is reason to believe the IRS will be more frequently targeted in the future. After all, the IRS stores highly sensitive information on each and every American taxpayer, from individual taxpayers to large organizations, and from mom-and-pop businesses to multinational corporations. The challenge of data security matters a great deal to every single taxpayer and will continue to be a central challenge to tax administration in the coming years.

Of course, data security and the protection of taxpayer information are of the highest importance in the prevention of stolen identity refund fraud. Identity theft, and the resulting tax fraud, costs taxpayers billions of dollars every year, and, once it occurs, it can take months or years for a taxpayer to mitigate the damage.

It was out of concern over stolen identity refund fraud that Ranking Member Wyden and I quietly launched an investigation earlier this year, requesting information and documents from the country's largest tax return preparers and debit card companies.

We look forward to working with the IRS as we move forward with this investigation and consider policy changes. We also look forward to hearing the report from your preparer working groups, and the committee looks forward to weighing in on those matters in the near future.

So I welcome our witnesses today, IRS Commissioner Koskinen and Inspector General George. Commissioner Koskinen, earlier this year, when I first welcomed you before the committee as chairman, I noted that I hoped it would be the beginning of a new chapter in the long, historic relationship between the Internal Revenue Service and the Senate Finance Committee. I said that because the

issues before us are too great for that relationship to be anything but open, honest, and productive.

Today's topic is a great example of why that relationship is so important. Cyber-threats will only continue to grow, and those types of threats go to the core of our voluntary tax system. We must work together to figure out what really has happened, what went wrong in allowing the breach to occur, and how we can prevent another successful attack from taking place in the future.

Finally, I would like to acknowledge that today's hearing occurs during somewhat unusual circumstances. The issue before us is the subject of several recently opened investigations, including a criminal investigation conducted by TIGTA. I caution members of the committee to be sensitive to these investigations when asking questions of the witnesses and be aware that they may not be able to provide full answers to every question in this public forum. In spite of these limitations, it is important to discuss this matter today as fully and candidly as possible.

[The prepared statement of Chairman Hatch appears in the appendix.]

The CHAIRMAN. With that, I would like to turn to Senator Wyden for his opening remarks.

OPENING STATEMENT OF HON. RON WYDEN,
A U.S. SENATOR FROM OREGON

Senator WYDEN. Thank you very much, Mr. Chairman. Mr. Chairman, I look forward to working with you and all our colleagues on what is another important and bipartisan concern for this committee.

Three months ago, the Finance Committee met in a hearing on the latest ID thefts and other scams plaguing taxpayers, and I said then that that wave of attacks sure looks to me like organized crime. Today, we meet after 104,000 tax returns have been hoovered up by what appears to be a sophisticated organized crime syndicate.

The problem continues to spiral, with hackers targeting Federal agencies, State governments including my own, and private companies alike, to steal money and data. One report from the Department of Homeland Security said Federal agencies' computer systems come under attack hundreds of times a day, tens of thousands of times a year.

The investigation of the stolen tax returns is ongoing as of this morning. But once again, it seems that the thieves are a step ahead of the authorities. They gained access to enormous amounts of personal data, which is up for purchase at extraordinary cost in the Internet's shadowy corners. These rip-off artists used that data to slip past the security filters at the IRS and steal taxpayers' most sensitive financial information. So it is my view that it is fair to say once again that this conduct fits the definition of "organized crime."

The thieves who steal taxpayer information could wipe out people's life savings and leave them in financial ruin. They could falsify tax returns next year or further down the road. They could take out huge, fraudulent home or student loans. And on a bigger scale, the money stolen in this cyber-crime wave could be funneled

into yet more criminal activity. It could wind up in war zones. There is a possibility it could be used to fund acts of terror without being traced.

Just like when the White House and the Department of Defense were targeted in the past, this was an attack on the security of Americans. I will be very direct about what is needed here. To protect taxpayers from this onslaught of cyber-crime, the IRS needs a 21st-century IT system.

Now, this is not just a question of resources, and it is certainly not a lack of commitment from the IRS staff. It is also a question of expertise. The era of punch cards and paper forms ended long ago. Federal agencies like the IRS need to tap into the expertise of our leading technology firms, our leading web firms—the pros who serve not millions or tens of millions but hundreds of millions of users.

This expertise will allow the IRS to avoid the pitfalls of the past and to implement a 21st-century IT system that protects taxpayers' privacy, catches the hackers and the cheats, and funds our government as efficiently as possible. When that system is in place, the Congress has to step up and provide the funds necessary to manage those functions effectively.

Legislators would not call for the Department of Defense or White House security budgets to be slashed after cyber-attacks, but the IRS's security funding has been shrinking for years. No company would try to defend against modern cyber-criminals with technology that is 20 or 30 years old, but that is what the IRS is stuck using in the absence of the expertise and resources to serve the American taxpayer.

The Congress must also make sure that the IRS has the information it needs to mount the strongest possible fight against the fraudsters. If the IRS had access to the data on W–2 and 1099 forms from the beginning of tax season, it would be much easier to catch fraudulent returns early and save taxpayers the nightmare of a stolen refund. Chairman Hatch and I have developed a bipartisan proposal to add an extra level of security by expanding the program that distributes unique passwords for individual taxpayers to use when they file. And when the taxpayer does become a victim of fraud, they ought to get more help undoing the damage more quickly and restoring their credit.

It ought to be clear to all that beefing up cyber-security at the IRS ought to be a top priority and draw on the technology expertise that exists in my home State and in States across the land. It is my hope that our hearing today will set aside once again the politics of these issues and focus on bipartisan, fresh ideas of how to best protect our taxpayers.

Thank you, Mr. Chairman, and I look forward to working with you.

The CHAIRMAN. Thank you, Senator.

[The prepared statement of Senator Wyden appears in the appendix.]

The CHAIRMAN. Our first witness today is IRS Commissioner John Koskinen. Commissioner Koskinen has been serving as the head of the Internal Revenue Service since December 2013. Mr. Koskinen's extensive public- and private-sector experience has pre-

pared him to confront the many challenges facing the IRS. I have a great deal of confidence in Commissioner Koskinen.

I want to thank you, Commissioner, for being here with us today.

Let me introduce our second witness as well, and then we will have you give your statements.

Our second witness today is Inspector General Russell George, the Treasury Inspector General for Tax Administration, or TIGTA. Inspector General George has been serving as the head of TIGTA since 2004. Mr. George has extensive public-sector experience, including working for the House of Representatives' Committee on Government Reform and Oversight.

I have a great deal of respect for you also, Mr. George, and I want to thank you, Mr. Inspector General, for being here today.

So if you will, Commissioner Koskinen, we will start with you. We hope you can keep your remarks within 5 minutes, because I am sure we are going to have a lot of questions.

STATEMENT OF HON. JOHN A. KOSKINEN, COMMISSIONER, INTERNAL REVENUE SERVICE, WASHINGTON, DC

Commissioner KOSKINEN. Chairman Hatch, Ranking Member Wyden, and members of the committee, thank you for the opportunity to appear before you today to provide information on the recent unauthorized attempts to obtain taxpayer data through the IRS's Get Transcript online application.

Securing our systems and protecting taxpayer information are top priorities for the IRS. Even with our constrained resources as a result of repeated decreased funding over the past few years, we continue to devote significant time and attention to this challenge. At the same time, it is clear that criminals have been able to gather increasing amounts of personal data as the result of data breaches at sources outside the IRS, which makes protecting taxpayers increasingly challenging and difficult.

The unauthorized attempts to access information using the Get Transcript application were made on approximately 200,000 taxpayer accounts from questionable e-mail domains, and the attempts were complex and sophisticated in nature. The attempts were made using taxpayers' personal information already obtained from sources outside the IRS.

It should be noted that the third parties who made these unauthorized attempts to obtain tax account information did not attempt to gain access to the main IRS computer system that handles tax filing submissions. The main IRS computer system remains secure, as do other online IRS applications such as "Where's My Refund?"

To access Get Transcript, taxpayers must go through a multistep authentication process to prove their identity. They must first submit personal information, such as their Social Security Number, date of birth, tax filing status, and home address. The taxpayer then receives an e-mail from the Get Transcript system containing a confirmation code that they enter to access the application and request a transcript.

Before the request is processed, the taxpayer must respond to several so-called out-of-wallet questions designed to elicit informa-

tion that only the taxpayer would normally know, such as the amount of their monthly mortgage or car payment.

During the middle of May, our cyber-security team noticed unusual activity on the Get Transcript application. At the time, our team thought this might be a "denial of service" attack, where hackers try to disrupt a website's normal functioning. They ultimately uncovered questionable attempts to access the Get Transcript application.

Of the approximately 100,000 successful attempts to access the Get Transcript application, only 13,000 possibly fraudulent returns were filed for tax year 2014, for which the IRS issued refunds totaling $39 million. We are still determining how many of these returns were filed by actual taxpayers and which were filed using stolen identities.

For now, our biggest concern is for the affected taxpayers to make sure they are protected against fraud in the future. We have marked the accounts of the 200,000 taxpayers whose accounts were attacked by outsiders to prevent someone else from filing a tax return in their name, both now and in 2016. Letters have already gone out to the approximately 100,000 taxpayers whose tax information was successfully obtained by unauthorized third parties. We are offering credit monitoring at our expense to this group of taxpayers. We are also giving them the opportunity to obtain an Identity Protection Personal Identification Number, or IP PIN as it is known. This will further safeguard their IRS accounts.

We are also in the process of writing to the 100,000 taxpayers whose accounts were not accessed to let them know that third parties appear to have gained access from outside the IRS to personal information such as their Social Security Numbers and other information. We want them to be able to take steps to safeguard that data. The Get Transcript application has also been taken down while we review options to make it more secure without rendering it inaccessible to legitimate taxpayers.

The problem of criminals using stolen personal information to impersonate taxpayers is not a new one. The problem of tax refund fraud exploded from 2010 to 2012. Since then, we have been making steady progress both in terms of protecting against fraudulent refund claims and prosecuting those who engage in this crime. Over the past few years, almost 2,000 individuals were convicted in connection with refund fraud related to identity theft.

Additionally, as our processing filters have improved, we have also been able to stop more suspicious returns at the door. This past filing season, our fraud filters stopped almost 3 million suspicious returns before processing, an increase of over 700,000 from the year before. But the criminals continue to become more sophisticated and creative. For that reason, as the chairman noted, we recently held a sit-down meeting with the leaders of the tax software and payroll industries and State tax administrators. We all agreed to build on our cooperative efforts of the past and find new ways to leverage this public-private partnership to help battle identity theft. We expect to announce more details shortly.

Congress plays an important role too, and can help by approving the President's 2016 budget request, which provides for $101 million specifically devoted to identity theft and refund fraud. And as

Senator Wyden noted, a key legislative request, among others in the budget, is a proposal to accelerate information return filing dates generally to January 31st of the year following the year for which the information is being reported. That would assist the IRS in identifying fraudulent returns and reduce refund fraud related to identity theft.

Chairman Hatch, Ranking Member Wyden, and members of the committee, this concludes my statement, and I would be happy to answer your questions.

[The prepared statement of Commissioner Koskinen appears in the appendix.]

The CHAIRMAN. Well, thank you, Mr. Koskinen.

I will turn to Mr. George.

STATEMENT OF HON. J. RUSSELL GEORGE, TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION, DEPARTMENT OF THE TREASURY, WASHINGTON, DC

Mr. GEORGE. Thank you, Chairman Hatch, Ranking Member Wyden, members of the committee. Thank you for the opportunity to discuss the data breach that occurred at the Internal Revenue Service.

On May 26, 2015, the IRS announced that criminals had used taxpayer-specific data acquired from non-IRS sources to gain unauthorized access to information on approximately 100,000 tax accounts through the IRS's Get Transcript application. Our Office of Investigations continues to investigate this incident, coordinating with other Federal enforcement agencies.

According to reports we received from the IRS, which we have not yet validated, an individual or individuals succeeded in clearing an authentication process that required knowledge of prior information about the taxpayer, including Social Security Number, dates of birth, tax filing status, street addresses, as well as answers to personal identity verification questions that typically only the taxpayer would know.

Security of taxpayer data has been designated by TIGTA as the top concern facing the IRS since fiscal year 2011. Due to the significant risks in this area, we currently have an audit underway to assess the IRS's processes for authenticating taxpayers at the time the tax returns are processed and when accessing IRS services.

Information obtained from data breaches in recent years and increased availability of personal information on the Internet have resulted in a weakening of controls used to authenticate individuals accessing personal data. The risk for this type of unauthorized access to tax accounts will continue to grow as the IRS focuses its efforts on delivering taxpayers' self-assisted, interactive online tools. More avenues for online assistance also mean more opportunities for exploitation by hackers and greater risk to the IRS and taxpayers.

In prior audits, we have identified a number of areas in which the IRS could better protect taxpayer data and improve its overall security posture. For example, we found that the IRS had not always applied high-risk computer security upgrades, known as

"patches," to help ensure IRS systems were protected and operated securely.

In another audit, we found that the IRS office responsible for addressing cyber-attacks was not monitoring a significant percentage of IRS servers, which puts the IRS's networks, data, and applications at risk.

The IRS is continuously under attack by those using the tax administration system for personal gain in various ways. These attacks and the methods used to perpetrate them are constantly changing and require constant monitoring by the IRS. Two of the most pervasive frauds currently being perpetrated that impact tax administration are the phone impersonation scheme and identity theft.

In summary, the IRS faces the daunting task of protecting its data and IT environment from the ever-changing and rapidly evolving hacker world. This incident that is the subject of the hearing provides a stark reminder that even security controls that may have been adequate in the past can be overcome by hackers, who are anonymous, persistent, and have access to vast amounts of personal data and knowledge. The IRS needs to be even more vigilant in protecting the confidentiality of sensitive taxpayer data. Otherwise, as shown by this incident, taxpayers can be exposed to the loss of privacy and to financial damages resulting from identity theft or other financial crimes.

We at TIGTA are committed to our mission of ensuring an effective and efficient tax administration system and preventing, detecting, and deterring waste, fraud, and abuse. As such, we plan to provide continuing audit and investigative coverage of the IRS's efforts to effectively protect sensitive taxpayer data and investigate any instances of attempts to corrupt or otherwise interfere with tax administration.

Chairman Hatch, Ranking Member Wyden, and members of the committee, thank you for the opportunity to share my views.

[The prepared statement of Mr. George appears in the appendix.]

The CHAIRMAN. Well, thank you, Mr. George.

Let me start with you, Inspector General George. In your written testimony, you said that TIGTA has designated the security of taxpayer data as the top concern facing the IRS in every year since 2011, as you stated here today. But in spite of your concerns, the IRS has not implemented many of TIGTA's audit recommendations about how the IRS can strengthen its IT security.

You noted that as of March 2015, the IRS had not implemented 44 of TIGTA's audit recommendations about information technology security, 10 of which were more than 3 years old. Beyond that, the IRS had disagreed with another 10 recommendations about IT security.

Mr. Inspector, if the IRS had fully implemented TIGTA's past recommendations about IT security, do you believe that the recent attacks on the Get Transcript application would have been successful?

Mr. GEORGE. I cannot at this stage, Mr. Chairman, give you a definitive answer as to whether or not it would have been possible. But I can say it would have been much more difficult had they implemented all of the recommendations that we made.

The CHAIRMAN. Thank you.

Mr. Commissioner, in your testimony, you acknowledge that the use of stolen identities to perpetrate tax fraud has really exploded in recent years. Now, due to the theft of personal information from your agency, there are more than 100,000 new identities on the international black market, and as many as 13,000 new fraudulent returns have been filed, at a cost to taxpayers of up to $39 million.

When it comes to identity theft and tax fraud, I do not think we can adopt a "pay and chase" mentality, or we will lose every single time. Stolen identities are a significant problem, but also not a problem that your agency can solve on its own. What your agency can solve is the ease with which criminals then use this stolen information to obtain fraudulent tax refunds.

News reports indicate that the recent IRS identity thieves may have been in Russia. Two years ago, TIGTA found large numbers of fraudulent refunds issued to Bulgaria, Lithuania, and China.

Now, I am not asking you to speak about the new investigation, but can either of you tell the committee about what more can be done to stop these thieves from robbing the Treasury both at home and abroad? And do you feel like you have received the adequate cooperation of the Justice Department and others in finding and stopping these perpetrators?

Commissioner KOSKINEN. Well, it is, as noted, an increasingly complicated challenge everyone faces in the financial world. I would just note, as a correction, there are not 104,000 new stolen identities. Those identities were stolen before the transcripts were accessed. What is available now is, for those transcripts out there, more details to go along with those stolen identities, and that is part of the problem. As there are breaches across the private sector or across the economy, all of that data is being collected by organized criminals who have a database in what is the so-called dark net that exceeds the amount of data that is in the regular web that we all use. So it is, as the Inspector General says, an increasingly complicated challenge. What worked yesterday, what worked a year ago, may not be working anymore today. So you continually have to attack that problem.

We work very closely with the Inspector General and value their input, and, in fact, in many cases we ask them to do tests, to do reviews and audits of the security and the IT systems as we go forward.

In response to your question, we have looked at that in terms of the suggestions made about improvements we could make. Virtually all of the reports we have had recently have appropriately looked at our security with regard to our basic database. Those reports and those recommendations did not deal with the e-authentication process for this website. The problem with the e-authentication process for the website is, what was a perfectly good security mechanism that was used by private-sector financial institutions and others, as the Inspector General says, is being overtaken by events.

The CHAIRMAN. In too many cases, foreign criminals are reaching into the Federal Treasury from abroad. Now, do you get adequate cooperation from foreign governments?

Commissioner KOSKINEN. Well, we get very good cooperation from the Justice Department. As I noted, with our Criminal Investigation Division, and working with TIGTA, we have thrown almost 2,000 people in jail. Our resources there—we have 300 fewer criminal investigators than we had 4 or 5 years ago.

It is a problem when you find, as we do, that an increasing number of the attacks are coming from criminal syndicates in Eastern Europe and Asia. Extradition, finding, tracking those people down, is much more difficult, and, as a general matter, we do not get a lot of cooperation.

The CHAIRMAN. Okay. Senator Wyden?

Senator WYDEN. Thank you very much.

Commissioner, at a hearing in March, I pointed out that with the increased sophistication of those involved in taxpayer ID theft, it looked to me like the work of organized crime. I understand that you have since stated that most of taxpayer ID theft involves organized crime. You also said that the recent taxpayer ID theft involved bulk attempts to access taxpayer records.

Now, I know the investigation of this latest ID theft is ongoing, but from what I have seen thus far, it sure looks to me like this attack was undertaken by an organized crime syndicate that already had access to enormous amounts of data on U.S. taxpayers. Would you agree?

Commissioner KOSKINEN. I would. As I said, there is an unimaginable amount of personal data in the hands of criminals as a result of data breaches across the economy, not only here but criminal syndicates around the world, in Eastern Europe and in Asia. And the battle is becoming increasingly more difficult, not just for us but for everyone in the private sector. In many ways, this event is a shot across the bow to remind people of the nature of the battle we are fighting and the sophistication of the enemy.

Senator WYDEN. And would you then say, given that you said you agreed with my description of the threat, that your challenge is making sure you are in a position to have a game plan so you can stay ahead of these increasingly sophisticated threats to our taxpayers?

Commissioner KOSKINEN. Right. Whether we are ever going to be able to stay ahead or not is the challenge. Our goal right now is to try to make sure that we are at least even with them in understanding what is going on and being able to protect taxpayer data and taxpayers from these ongoing attacks.

Senator WYDEN. Let us talk for a few minutes then about the game plan that you would have to have. As I say, I think the sophistication of these organized crime syndicates is such that, whenever you close this door, they look for the next one, and that is why I talked about how we are going to try to take them on.

It seems to me it comes down to having the people who have the skills and experience to combat the threats, the critical pay authority to be able to hire them, and sufficient funding to upgrade the IRS computer security systems.

Are those generally the elements of the kind of strategy that you want to have?

Commissioner KOSKINEN. Those cover most of the significant points, particularly what we call the streamlined critical pay. It is

a small number of people whom we are authorized to hire, but it allows—our present head of Information Technology is on streamlined critical pay. That program worked for about 14 years, but it was not extended 2 years ago. I was just talking to our IT head. We had two very senior, sophisticated IT people we could not hire because they did not want to go through the normal government process.

So it is critical to us. It is a total authorization of 40. We had 29 when I started; we are down to 16 as that program runs off. A key member of our cyber-security unit is on critical pay. Our Online Services Program Director was hired through streamlined critical pay authority. So that authority is critical for the small number of people we need who are going to be world-class experts at dealing, not only with technology, but with security.

Senator WYDEN. What does this committee need to do—because you have heard Chairman Hatch and I indicate we want to work with you on a bipartisan basis to address this. What does this committee need to do to assist you in executing this game plan to make sure, for example, you have an adequate number of people in cyber and these kinds of issues?

Commissioner KOSKINEN. Well, I appreciate the chairman's note that we need to work on this together. This is not an issue that has a political overtone to it. This is a challenge that faces every American, faces every company in this country.

As I noted, if we could get W–2s and information returns earlier, it would allow us to be more effective in protecting against identity theft. To the extent that we could get authority to, in fact, adjust the way Social Security Numbers are produced on W–2s, it would help us ensure that those W–2s are not fraudulent.

There are other legislative supporting issues, including streamlined critical pay, that would be very helpful. And, obviously, I think the chairman is right. We have not made a point in this presentation that budget is an issue, but we are running an antiquated system with some applications that are 50 years old. In some cases, as the IG noted, we have not even been able to provide patches for all of the upgrades. Some of our systems do not have patches because they are no longer supported by the providers.

So we obviously do need jointly to figure out what it takes to make sure that this system is able to protect people.

Senator WYDEN. Commissioner, thank you. It just is clear to me that if you have IT from the Dark Ages, you are not going to be able to stay on top of these kinds of problems. So I am committed to working with you, and I also mentioned in my opening statement there are some very good people in the technology sector, people who run major tech firms, whom I think would also be available to work with you all. So we are committed to making sure that you understand there is a bipartisan effort to help you put that game plan in place.

Thank you, Mr. Chairman.

The CHAIRMAN. Thank you.

Senator Grassley?

Senator GRASSLEY. First of all, Mr. Koskinen, I thank you for coming for this conversation, and the reason for that is that the theft of personal private tax information of over 100,000 taxpayers

is deeply concerning, because our whole tax system is based on the proposition of voluntary compliance and privacy and all that.

So I am asking about a letter I sent to you asking a number of questions related to the data breach, and I do not expect those answers now, but I want to find out when I am going to get answers to my letters. This would include requests for documents that should shed light on whether the IRS carefully considered security risks prior to instituting the Get Transcript online service. My letter asks that you provide a response by June 4th, and it was sent last week.

Some examples of what we are concerned about are whether or not you had a risk assessment plan, an implementation plan, and mitigation plans. Those are some of the documents I am asking for.

Do you have any idea where my request stands in the process? And do you expect to be able to fully respond to my letter by June 4th? And if not, when do you expect that I would be able to get a response?

Commissioner KOSKINEN. That is a good question. As you know, and as I committed to the chairman at my confirmation hearing, we treat letters from the Hill very seriously. They are a high priority. Sometimes we get a request to give a response within a week to a lot of data that is difficult for us, but our goal is to, in fact, not delay this any longer than necessary.

The amount of information you want probably makes it unlikely we will get it by the end of this week, but certainly by next week we expect to be able to provide you that data. The chairman has a pending request to us, a very thoughtful request, about our entire IT program, which is in the process of coming back to him. It has taken longer than we would like, but it is going to be 40 or 50 pages long, with very, I think, instructive detail—I found it interesting to read—about the priorities we have, the challenges that we have faced over time, and how we have responded to those.

But we will point out to you that we take risk seriously. When this Get Transcript was put up, when any new application is put up, we look at the security risks. Whenever we have a new program, we work with the Inspector General to see that it is being set up appropriately, that there are appropriate protections.

And so, it is an important question, one that, as we move along—not only do we have risk mitigation plans when we start, we monitor as we go forward each year what are the schemes, what is going on with identity theft, where are the attacks coming from. We are pinged, as it were—not necessarily attacked but just people checking to see where we are and what they might be able to find—over a billion times a year. So we have security going on every day.

The CHAIRMAN. If I can interrupt, we have a vote on. Senator Grassley will finish his questions, and then next is Senator Carper. And I will try to get back by then. If not, after Senator Carper is Senator Enzi.

Senator GRASSLEY. Okay.

The CHAIRMAN. So, in that order.

Senator GRASSLEY. Yes. Well, I think I heard you say that you will fully respond. It may not be by June 4th but next week. Thank you.

Mr. George, IGs are very important offices as far as I am concerned. Did your office evaluate the security measures put in place by the Get Transcript service either before or after it went online? And if so, what were your office's findings? Did the IRS fully comply with any recommendations you may have made?

Mr. GEORGE. Mr. Grassley, we did take a look at an earlier iteration of the Get Transcript program and at that time made some recommendations that we believe were implemented. We have not taken a look at a subsequent version of it until now. But obviously we will be looking at that.

Senator GRASSLEY. Okay. Mr. Koskinen, reportedly the attacks began in mid-February, but the IRS failed to notice suspicious activity until mid-May. Why was the IRS not able to detect the malicious activity when it initially began?

Commissioner KOSKINEN. Last filing season, there were 23 million successful downloads on the Get Transcript application, so it is a huge volume. We now know when it started by going back through our logs. We log every transaction. They were shrouded under the huge volume of requests going out legitimately.

When the filing season ended, I think what happened was that the volume dropped—not "I think." I know it dropped, and then it suddenly started up again. But, by that time, the volume of legitimate requests had dropped, and the activity became visible to us. I am not sure that people expected it to be visible, but anyway, that was when we found it. It was in mid-May when we noticed it. As I say, first we thought it was a denial of service attack, because things were backing up in a way that was unexpected. Within a couple days, our security people went through and figured out it was not that; it was, in fact, unauthorized attempts to access the data. And as soon as they found that out, within a day or two they sat down with us. We advised the Hill, and as I say, I am delighted that we have been able to notify the 104,000 taxpayers already.

Senator GRASSLEY. My time is up. Thank you.

Senator CARPER. Thanks, Mr. Chairman. Gentlemen, welcome. It is great to see you both. We appreciate your presence today. We appreciate very much your service to our country.

I want to start off by going back to Commissioner Koskinen talking about what the IRS is doing in reaching out to those citizens, those taxpayers whose information has been or may have been compromised to try to help them in a time of uncertainty and probably a time of considerable concern and worry.

A lot of us use the Golden Rule to kind of guide us in our lives: treat other people the way we would want to be treated. Tell me how the IRS is, if you will, using the Golden Rule to reach out to the people whose information may have been put at risk, or has been put at risk.

Commissioner KOSKINEN. The investigation is still going on by ourselves, by the Inspector General, but one of our concerns was, as soon as we knew that there had been inappropriate access and data had been released, our first concern was taxpayers. We regret that this attack took place. We understand that it is a traumatic event for taxpayers. We work with taxpayers as victims of identity fraud every filing season, virtually every day.

So our goal was, even while we were trying to get to the bottom of it, once we were able to identify the taxpayers whose information had gone out, our goal was to get that notice to them as quickly as we could. We secured their accounts—we secured the accounts of the other 100,000 even though no data went out—so that there would not be false refunds available to be filed against their Social Security Numbers.

As I say, we have completed the mailings to the 104,000. We are offering them, at our expense, credit protection. We are also offering them the option to authenticate themselves and get an Identity Protection PIN, or an IP PIN, to give them even further security as they go forward.

So we have done everything we think we can do, and most importantly, we have done it as quickly as we could, because we think it is important for them to have that information.

Senator CARPER. Thank you. Just very briefly, did you say the letters have been sent or are being sent?

Commissioner KOSKINEN. The letters are all in the mail.

Senator CARPER. And when would you expect——

Commissioner KOSKINEN. The letters for the 104,000. We are now processing the letters to the 100,000 where no data escaped, but we think they need to be notified that we have evidence that criminals have access to their personal information.

Senator CARPER. Do those letters include phone numbers that people can call to have further conversation and gain some further assurances?

Commissioner KOSKINEN. There are numbers to call, although, as you know, the ability to get us on the phone is not as good as we would like it to be, so we have posted information on our website. We are suggesting they go to the website first if they have questions. And we have already had some people showing up at our Taxpayer Assistance Centers, and we are providing them assistance as well.

Senator CARPER. All right. Sometimes people ask me why I have had some success in my life. I always say, "I have always surrounded myself with people smarter than me." My wife has often said, "It is not hard to find them." But I want to talk about—I want to go back to the issue of streamlined critical pay.

I would like for us to think—and I will ask you to answer for the record. If we were to restore this program, which I think ended in 2013——

Commissioner KOSKINEN. Yes.

Senator CARPER. If we were to fully restore and fund this program, what would be the cost of that on an annual basis? Compare that for us with the cost of this breach. What is this costing the Treasury as we attempt to respond to it, at least to date? You do not have to do that right now, but if you have it off the top of your head, that would be fine. I would love to know what kind of return we would get on the investment if we were to restore this program.

Commissioner KOSKINEN. The Inspector General did a review of the program that he published last December, and, as a general matter, it appeared that the cost to the Government was $400,000 or $500,000 a year, because, you know, the pay increase differential is relatively modest. We only had about 30 people who had taken

advantage of it. And some of them get paid less than senior SESers. So for the $400,000 or $500,000, we think you get a great return. As I say, the 13 million returns that went through with refunds out of the 104,000 have refunds totaling $39 million. Now, some of those will turn out to be real taxpayers, but obviously the return on the investment is significant.

As I said, the head of our IT program, who is wonderful, is a streamlined critical pay guy. We lost the three people who were great data analytics people, including an expert on authentication.

Senator CARPER. Thank you. Inspector General, can you give me a number, 10 to 1, 50 to 1?

Mr. GEORGE. I do not know that we have a number.

Senator CARPER. I am going to ask you to just respond to that for the record, if you would.

Mr. GEORGE. We will, to the extent that we can, but I would say that we did find that the program was operated successfully, and it was justified.

[The information appears in the appendix on p. 44.]

Senator CARPER. Okay. Thank you.

Outside help—you are not in this by yourself. You have other Federal agencies that have responsibilities to be of assistance to you at the IRS, and one of those is the Department of Homeland Security. I would just ask you for the record what help have they provided, and is there more that they and other agencies should be doing?

Commissioner KOSKINEN. We have regular communications with Homeland Security. I have met with the Secretary of Homeland Security, actually at your suggestion. They provide us technical expertise. We alerted them immediately, even when we thought it was just a denial of service attack, that this was an issue they needed to know about. We alerted the Inspector General.

Homeland Security has been very supportive, and what they provide is updated information about what they are seeing across the spectrum. So there is a good working relationship across the Government of agencies under attack trying to see what are the patterns, what is going on, and what can we learn from each other.

Senator CARPER. All right. Thank you both very much.

Senator Enzi?

Senator ENZI. Thank you, and thank you, Mr. Commissioner and Mr. Inspector General, for being here. I read your testimony. I thought of some other possibilities for the data breach, and I was reminded of them when I filed my taxes. I had overpaid, and I do not have electronic transfer to the bank, because I am not going to share that information with the IRS or anybody else. So I received my tax refund in an envelope, of course, a paper check, and what surprised me was, in the envelope there was also a flier from the Consumer Financial Protection Bureau.

Now, the Consumer Financial Protection Bureau has the power to examine and impose reporting requirements and all kinds of regulations on financial institutions and on personal information. They are collecting everything. People are worried about the National Security Administration. They ought to worry about the Consumer Financial Protection Bureau. They are getting all of our

data all of the time, and that is one of the possibilities for a security breach.

I do not believe the authority extends to the IRS to solicit Americans' stories about their money through the Consumer Financial Protection Bureau. Additionally, since the Consumer Financial Protection Bureau is funded by a transfer of non-appropriated funds from the Federal Reserve System's combined earnings before it ever gets to the general fund, I question whether it is appropriate to use taxpayer dollars to advertise the Consumer Financial Protection Bureau as the IRS did by including this mailing with the tax refunds.

And, lastly, because the CFPB is supposed to be an independent organization, I do not believe the Treasury Department should be soliciting information on behalf of the entity. So I would appreciate answers to the following questions. Some of these will be more detailed than the time that we have for them, but I would like to know what authority the Treasury Department relied on to include that information in the IRS tax refunds. What agency paid to print and mail those fliers? Have you respected all the boundaries concerning confidential taxpayer information? Could hackers be getting data from the Consumer Financial Protection Bureau that is used with the IRS from data that maybe the IRS is sharing with that department?

Mr. Commissioner, could you—some of those I will put in more detail for written answers, but my best chance of getting an answer is right now. So how did that happen to wind up in my statement?

Commissioner KOSKINEN. I am delighted to respond. First, I should make a correction to the record. I just talked about 13 million returns. It is 13,000 returns had a false refund, potentially false refund. There may have been real taxpayers in my previous question.

With regard to this, we often provide taxpayers with information that may be of interest or support to them, particularly in financial matters. We do not share—under our protection of taxpayer data—information with other Federal agencies unless there is a specific statutory authorization for that, and to my knowledge, there is not one with the Consumer Financial Protection Bureau.

I will be happy to get you further details as to who paid for the flier, why it was put in there. Generally, if we provide information to taxpayers, it is for their assistance, for their information, in ways that may be helpful to them. We are not asking for them to provide us additional information in those filings, but we will get you more detailed information, and I will get you that answer, again, if you will provide the detail of that question. Do not wait for the record. If you will just send me a note, I will get you the answer back quickly.

Senator ENZI. Okay. I will be asking you some questions about that, because I know there is even a cost to putting something in an envelope.

A different question. Some unlicensed tax return preparers maybe are preying on uninformed taxpayers, and I did not exactly see that in the testimony, but I know that is one of the possibilities for places where people may be getting the information. To what

degree is the IRS working to eliminate these fraudulent taxpayer return people?

Commissioner KOSKINEN. We monitor tax preparers. We have actually had criminal prosecutions against a number that have taken advantage of their clients. We are concerned about, not only criminal tax preparers, but uninformed tax preparers, and, as you know, we requested legislation that would allow us to require minimum qualifications for a tax preparer. If you go into particularly low-income or immigrant communities, you will see people advertising, "Come with us. We will get you a big refund." They do not say, "Whether you are entitled to it or not," but that is basically what they are up to.

And so, to the extent we can, we have a voluntary program that provides continuing education for tax preparers who want to sign up, but we do monitor fraudulent returns, and, if there is a pattern that they come from an individual preparer or group of preparers, we refer those cases for prosecution.

Senator ENZI. Thank you. I appreciate you being here.

The CHAIRMAN. Well, I think I might as well ask a couple questions. But first we will go to the senior Senator from Kansas.

Senator ROBERTS. Well, thank you, Mr. Chairman.

Gentlemen, thank you for coming. Thank you for endeavoring to get to the bottom of this and come up with some answers.

I must tell you, just the other day, when coming back to Washington on an airplane from Kansas, somebody leaned over and said, "What is this business with the IRS?" And I responded with regards to what I thought was his concern with regards to the ongoing targeting of conservative groups applying for exempt status. He says, "No, no, no, no, no. There has been an attack." I said, "Oh, well, we have a breach. We have a cyber-attack." He said, "Well, what was that all about?" And I said, "Well, we do not know yet, but we are going to have a hearing, and I know we can try to get to the bottom of it. But what we do know is that this is a foreign hacker, probably from Russia, probably Russian mafia." There was a long pause, and he looked at me, and he said, "I do not really have anything more to say." So this whole thing just rendered him speechless, and I think a lot of people are in the same boat. And it is a paradox of enormous irony.

My staff tells me that just prior to this breach, privacy experts went in to brief them weeks ago, just weeks ago, on how safe data was contained in the Get Transcript system and how it was safe, and that is a "was" now, not an "is."

I do not think this is a new threat. I know it is not to both of you. The agency, the Inspector General, the GAO, and the committees with oversight have been concerned about these threats for years. GAO reported this March that the data under the control of the IRS is "unnecessarily vulnerable to inappropriate and undetected use."

I agree with Senator Wyden. There is a war going on. On one side we have the government, taxpayers, and business, and on the other, hackers and criminals, organized syndicates, some lone wolves, perhaps even national governments. Right now, it looks like we are losing this war, so we certainly need to use this latest breach to consider how we can regroup and win the fight.

My concern is whether the IRS has the tools and mind-set to achieve better security and whether it is even capable of safeguarding this core function. I am very concerned that, in a rush to push out programs like Get Transcript—albeit this was pushed out some time ago—we have let access and purported cost savings overtake the absolute need to safeguard taxpayer information.

So to the Honorable John Koskinen, thank you for coming, sir. To what extent do you partner with the private sector on data security? Do you need any additional flexibility or authority to work with outside experts to make sure you have access to the tools and the technology to address the privacy and also the data security issues?

Commissioner KOSKINEN. We have an ongoing partnership with various elements of the private sector. We have a great working relationship with financial institutions that work with us on stopping improper refund payments. As I noted, we pulled together 3 months ago what we call a "Security Summit," where I asked the CEOs of the major tax preparers, tax software providers, and State tax administrators to sit down with us, and I told them when we started: "The purpose of this meeting is not for me to tell you what we are going to do or what you ought to do. The purpose of this meeting is to start a partnership where we work together to figure out how the three of us—the private sector, States, and the Internal Revenue Service—can work together in the battle.

Senator ROBERTS. Is that ongoing?

Commissioner KOSKINEN. And that is ongoing. We expect probably next week to give a public discussion of what we are going to do for the next filing season. But I told them it is not just for the next filing season. We need to begin to take a look at, on a longer-term basis, what are the things we need to do.

One of the issues we may need to discuss, although we think we have the authority, is the private sector noted that they need a level playing field, so if we come up jointly with requirements as to sharing of data or the implementation or what we are going to require from taxpayers, we are the only ones who can require that across the board so that one person is not getting an advantage. And we will do that if necessary, and, if we need legislation, we will be back. But thus far, it has been a wonderful working relationship.

Senator ROBERTS. I appreciate that. My time is running out. I just have one more question for Mr. George. I understand the IRS has shut down the Get Transcript program for the time being, and this hack has been stopped. But in looking at this program moving forward, how should we close the door to future attacks? How will you know that we have even succeeded in shutting the door?

Mr. GEORGE. Great question, Senator. I do not have a definitive answer at this time. As the IRS is attempting to make the experience between the taxpayer and the IRS more user-friendly, they are giving people opportunities to access information in ways that heretofore did not exist. It is a true challenge for the IRS to strike a balance between ease of access and security.

Now, the private sector, as has been pointed out, has experienced these types of problems. They have adapted, acquired different systems that would allow people to further authenticate who they are.

There is a cost associated with doing that, and whether or not the IRS is in a position right now, resource-wise, to do that, I would defer to the Commissioner.

But, sir, if I may, Mr. Chairman, one thing I do want to clarify is, we are still again at the outset of this investigation, but there have been reports that this data breach originated solely from Russia, and I want to make it clear that is not the case. It is beyond Russia. So I just wanted to get that on the record.

The CHAIRMAN. When you say "beyond Russia," what do you mean?

Mr. GEORGE. That there are other domains—the domains are located in nations other than Russia, in addition to Russia.

Commissioner KOSKINEN. I would just note that our experience with the criminal syndicates we are dealing with is that they are not limited by national boundaries. They are, in fact, operating globally. They are located and headquartered oftentimes in one country or another, but they are not constrained by geographic locations. And so our experience is, analyzing the data of the Inspector General, this is coming from several different, perhaps organized—clearly, it was an organized attack—but our experience in looking at syndicates around the world is that they cooperate when it is in their interests, and they cross national boundaries very easily.

Senator ROBERTS. Mr. Chairman, it occurs to me that perhaps we could have something called a "National Security Agency" or something that could monitor this kind of data and then see how the phone calls come in. Something like that might——

The CHAIRMAN. Sounds like a good idea.

Senator ROBERTS. Yeah, it sounds like a good idea to me.

Could I simply ask that a *New York Times* article which contains a statement by Nina Olson, who leads the Taxpayer Advocate Service, an independent office at the IRS, be inserted in the record at this point? I apologize to my colleagues for going over time.

The CHAIRMAN. Without objection.

[The article appears in the appendix on p. 63.]

The CHAIRMAN. Now, before I go to Senator Isakson, have you pinpointed any country or countries from which this came?

Mr. GEORGE. Yes, but, again, we have to be careful because of the active investigation, Mr. Chairman. But as the Commissioner pointed out, you could be in Florida and you can use, you know, a router or a server in a different country on the other side of the world. I mean, eventually we are able to track them down, but at this stage, with the report that it was solely Russia, that is not accurate.

The CHAIRMAN. That was just a speculation, as far as I was concerned. But you are not in a position to name any country or countries?

Mr. GEORGE. At this stage, I would prefer not to publicly, but privately we would certainly share that information with you, Mr. Chairman.

The CHAIRMAN. Fine. Senator Isakson?

Senator ISAKSON. Thank you, Mr. Chairman. I would be happy to defer if you are in a hurry.

You know, I think it is ironic. Senator Roberts made an interesting observation, but for the last 6 days, the United States Senate has been debating the merit of whether or not 41 members of the NSA should have access to two phone numbers, the date of a call, and the duration of the call, without any personally identifying information whatsoever. We are getting ready to take that authority away from them, yet we have the Commissioner of IRS talking about 104,000 Americans who had their identities stolen. And when I file my tax return on April 15th, they know how much money I make, how much my wife makes, what church I go to, whom I give the money to, whether or not I had a casualty loss, where I buy stocks, where I buy bonds, where my money is deposited, and how much I owe on my house.

So I just want to put things in perspective, that this is an important hearing, but that information is a lot more private, a lot more personally identifying, and a lot more dangerous for the average American citizen than whatever the NSA ever does, and they are looking out for our physical safety. I just had to make that statement.

Secondly, it is ironic——

The CHAIRMAN. You summed that up very well.

Senator ISAKSON. Thank you. Experian just e-mailed me to tell me my credit card has just changed and I need to check with them on the potential of identity theft having taken place, and that just came in at 10:24 on my BlackBerry. I had mine stolen about 3 years ago, and I want to commend the Department, the Internal Revenue Service, for providing taxpayers whose identities have been breached with the right type of Experian or Equifax protection to see to it their identity is protected, just like mine is being protected because of the loss that I had.

I guess my question is on the IP numbers. Georgia is one of the States—there are three: the District of Columbia, Georgia, and I have forgotten the name of the other State where——

Commissioner KOSKINEN. Florida.

Senator ISAKSON [continuing]. Florida, where the IRS gave taxpayers the option to apply for an IP number, which is a self-identifying number for a tax return. Is that correct?

Commissioner KOSKINEN. That is correct.

Senator ISAKSON. And there are a million and a half of those IP numbers now issued. Is that right?

Commissioner KOSKINEN. A million and a half are issued to those who have been victims of identity theft. We have had the pilot program where we had a few thousand. We are trying to get more people—we are running it as a pilot to see what the costs would be and the burden would be. We have had a relatively modest take-up on that, but we are encouraging taxpayers to take advantage of it.

Senator ISAKSON. Have you found it to be a foolproof system yet, or is that why you are doing a test?

Commissioner KOSKINEN. We are doing the test primarily to see what the burden on taxpayers is and what the cost to the IRS is. It is foolproof to the extent that you do not lose it. What happens with Social Security Numbers is they are, you know, out in the world. They are used for children's identification in school. On

everybody's Medicare card is a Social Security Number. The IP PIN has no other use, so our experience thus far is we can authenticate to make sure that the taxpayer who gets the IP PIN is the legitimate taxpayer. If they keep it secure, there is no way anybody gets access to that number, and their returns, therefore, are safe.

Senator ISAKSON. It would seem to me that if the trial that you are doing in Georgia and Florida and the District works and does seem to be foolproof, you would give every American taxpayer the ability to apply for one of those. I mean, you would not want to make them take one for fear of some sinister government plot somewhere, but you would certainly give them all the opportunity to get one.

Commissioner KOSKINEN. Right. Our challenge, what we are looking at with the PIN is, if people lose it, we have a lot of people then—if we get, for instance, 50 million people with IP PINs and half of them lose them, we are going to end up with a tremendous amount of background noise just trying to make sure we get them the right PINs and replacement PINs. So that is one of the things we are looking at: how does it work when you have people who otherwise have not been victims sign up? But it is ultimately a way to go.

When we get down to the bottom of it, our analysis over 4 or 5 years is, authentication is going to turn out to be the key, whether it is authenticating you to get an IP PIN which allows you to get in—and that is what we are working on with the private sector and the States. We need to, together among all of us, have a way of sharing information about who is actually the customer. Are you who you say you are? When you call us, you know you are you, but then you wonder why we have to authenticate you to make sure you are not somebody impersonating you.

So it is a multifaceted approach we are taking, trying a lot of different things to figure out, again, as the chairman said, how we get even or get ahead of the game. Ultimately, we will never put them out of business. The goal is to make it so difficult and expensive that it is not worth their while.

Senator ISAKSON. Mr. George, I want to ask you a question. It would probably be unfair of me to ask Mr. Koskinen this question, although he is welcome to comment if he likes. But I have been thinking, as I listened to both of your testimonies, that the best way to protect taxpayer identity and limit fraud is to change the way in which we do our taxation.

There is a Georgian by the name of Neal Boortz who wrote a book called "The Fair Tax," which advocates going to a retail sales tax and eliminating the inheritance tax, the payroll tax, and the income tax. If you paid at the retail purchase a tax to the Federal Government to supplant those three taxes, would it not be a seamless protection against identity theft?

Mr. GEORGE. I cannot give you a definitive answer on that one, Senator. Suffice it to say the more information, the earlier the IRS gets it, and an easier way of doing taxes would assist the system overall, the taxpayers and what have you. But the various proposals, such as the ones that you mentioned, I am not certain whether they would have a direct impact on identity theft.

Senator ISAKSON. I am not necessarily selling the proposal, but what I am saying is, if I paid my tax to the Federal Government on a retail purchase and it was collected by the retailer, who does that for the States anyway, it would eliminate any of this self-identifying information, and the tax would end up being collected, which would be a protection against some of the identity theft.

Mr. Koskinen?

Commissioner KOSKINEN. I think that is right. If we did not deal with taxpayers individually, we would not have individual information.

The issue globally would still exist, as with your credit card, and that is: are criminals accessing enough personal information to access your bank accounts, your credit cards, your mortgage accounts? But from the standpoint of the IRS, if we were dealing with a system where we collected funds, the government collected funds, with a value-added tax or a fair tax or something that did not require individuals to register with us, almost by definition we would not have the risk of individual identity theft, because we would not have individuals identified.

Senator ISAKSON. Mr. Chairman, my time is up, but I want to thank Mr. Koskinen for taking the time to invite me to the Chamblee headquarters of IRS in Georgia and giving me a tour. I appreciate the connectivity that you have there. I appreciate what you are trying to do.

The CHAIRMAN. Thank you, Senator.

Senator Scott, we will call on you.

Commissioner KOSKINEN. I might just note that the irony of that visit, which our employees genuinely appreciated, was the Senator and I spent an hour on a briefing on identity theft.

The CHAIRMAN. Good. Senator Scott?

Senator SCOTT. Thank you, Mr. Chairman. Commissioner, Mr. George, thank you for being here this morning.

Commissioner, can you tell me how many South Carolinians have been affected or had information stolen by the breach?

Commissioner KOSKINEN. I cannot tell you that. As I said earlier, we have sent letters to the 104,000 whose data was accessed, so anybody in South Carolina should be getting a letter in the next few days. We can go back through and get you that information.

Senator SCOTT. That would be great.

Commissioner KOSKINEN. We have not segregated it by State at this point.

Senator SCOTT. Thank you very much.

Whenever I go throughout South Carolina, my constituents are incredibly concerned about the IRS. They really feel like your agency is the agency that truly has the power of intimidation. So when we hear about breaches, 104,000 folks violated by this breach, my citizens are incredibly excited and passionate and concerned about the activities at the IRS, and it did not simply start with the breach. It started when we had the conversation last time about groups being targeted because of their religious beliefs or their political doctrine. It flows into the Lois Lerner e-mails and the inability to figure out if you have or if you do not have the e-mails. It continues on down the road as they call during tax season and they

are unable to get someone to answer the phone, so they have these courtesy hang-ups.

It is consistent, as I talk to my constituents, that their concerns continue to grow, and this breach will only add more fuel to the fire for people who are absolutely petrified by the IRS. And now having their information exposed to criminal elements, criminal cartels, is even more disconcerting.

I would love to hear what it is exactly that you are doing in order to secure the IT at the IRS. And then, Mr. George, I have a question for you about the 19 recommendations that were made and only 8 were implemented.

Commissioner KOSKINEN. What we are doing is, for years now, security has been a high priority for us. We understand, particularly with identity theft, which is based on information stolen elsewhere and then used to file a false return, that that is a difficult and traumatic situation for taxpayers. So one of our highest priorities is making sure that, if that happens to a taxpayer, they get a prompt response from us.

As I have noted, we work closely with the Inspector General and GAO. We value their recommendations. In some cases, we have actually asked them to take a look at our systems and to make sure they are not breached. As I said, we get pinged, not necessarily attacked, over a billion times a year. So we are aware—no one at the IRS is under any illusions that we are not at risk—and so we spend as much time and effort and resources as we can focused on that. Anytime we make a change in a system, anytime we make a change in a new application, we look at the security aspects of it.

As the Inspector General said, we are balancing off trying to provide better taxpayer service. As you noted, with the resource constraints, we did not answer the phones at anything like the rate we would like to have. We had 23 million transcripts successfully downloaded last year. Those were requests, otherwise, taxpayers would have had to make either on the phone or in person.

So to the extent that we can provide better service to taxpayers, that is a high priority for us. But ultimately I take your point—we take it very seriously—that taxpayers have to feel they are going to get treated fairly, no matter who they are, no matter what organization they belong to, no matter who they voted for. And we have done everything we can. We have implemented all the Inspector General's recommendations in those regards, and I think it is important for taxpayers to know that we take their concerns seriously. They are ultimately our customers. We work for taxpayers. We do not work for anybody else.

Senator SCOTT. Thank you, sir. I will say that, from a resourcing standpoint, it appears that during the Obama administration about $5 billion has been dedicated to the IRS for IT. Under the Bush administration, the number was somewhere around $5.3 billion. So in the last decade or so, over $10 billion for IT, and it just does not seem like the type of security that we would anticipate and expect is there.

And I am running out of time, Mr. George, so, of the 19 recommendations that were made previously for corrective action, it appears that only 8 of those 19 were implemented, and perhaps

some were closed before they were fully implemented. Can you shed a little light on that for me?

Mr. GEORGE. I will in the amount of time that we have left, and I would ask for permission to supplement my response in writing.

Senator SCOTT. Thank you very much.

Mr. GEORGE. We have made a number of recommendations, actually a total of 44 recommendations, as of March of this year. Eighteen of those have been recommendations from security audits that have yet to be implemented.

Ten of those recommendations come from five security audits that were completed during fiscal year 2008 to 2012, so they are very dated. And there are a couple of examples of some of the oldest recommendations that we made that we think might have had some bearing on the IRS's ability, if not to stop, again——

Senator SCOTT. Can you name just one?

Mr. GEORGE. Certainly. The IRS should require system administrators and their managers to correct user account deficiencies identified during the audit. Managers need to periodically review and validate access to systems, limiting it to people who only have a need for that information.

Senator SCOTT. Mr. George, that does not sound like a resource issue. That sounds like a management issue.

Mr. GEORGE. I agree, sir. I agree there.

Senator SCOTT. Okay.

Mr. GEORGE. I agree. And if I may add just one factoid, sir, that I just think is important to point out. The 104,000 figure is used a lot. We have to keep in mind those are the records, the transcripts that were accessed. A lot more people could be affected by that, because spouses and dependents of the taxpayer, their information is contained within those reports. So at this stage, again, I cannot give you a definitive number, and I do not believe the Commissioner is in a position to do so either. But it is more than 104,000 people certainly.

Senator SCOTT. Thank you, sir.

Mr. Chairman, thank you for the time.

The CHAIRMAN. Senator Casey, we will turn to you.

Senator CASEY. Mr. Chairman, thank you very much, and thanks for this hearing. Commissioner and Mr. Inspector General, thank you for your appearance here and your service. We appreciate it.

I want to start with the issue through the lens of Pennsylvania. We have had a number of reports—and I have heard directly from law enforcement in Pennsylvania—about identity theft, and not just the broad-based or the significant challenge it presents generally, but specifically because the response to it often involves many different agencies, for example, in addition to the IRS, the Department of Justice, the Social Security Administration, and State and local law enforcement.

So I would ask you first, Commissioner, about what we refer to as interagency and interstate coordination. Tell me about that in terms of what you have been able to do since you have been Commissioner.

Commissioner KOSKINEN. When all of this, as I said, exploded in 2010 to 2012, it overwhelmed law enforcement, overwhelmed everybody. Since then, we have established very successful partnerships

actually with State and local law enforcement across the country, particularly in States like Georgia and Florida where all of this seems to have started.

So they, together with our working relationship with the Department of Justice and U.S. Attorneys—we have a very active Criminal Investigation Division, but we do not prosecute people, we do not bring charges. So we have to work, again, in partnership with U.S. Attorneys across the country, and that has been a very successful and effective partnership. As I said, we have thrown almost 2,000 people in jail over the last few years who have been convicted and sentenced to long sentences as a result of those partnerships.

Senator CASEY. One of the realities of this for a State like ours—and I am sure this is true in other States as well—is local prosecutors, meaning District Attorneys, for example, at the county level, are among the law enforcement officials who have to confront the problem. So, Commissioner, I would ask for your commitment to work with our folks, both local officials and State officials, as well as taxpayers, on a coordinated approach to solve the problem.

Commissioner KOSKINEN. We are delighted to do that. We have no illusion we can do this by ourselves. We need as much help as we can get, and we have a great working partnership with the investigative arm of the Inspector General as well.

Senator CASEY. I appreciate that. Thank you for that commitment.

I want to turn to the question of resources. I know that often we in the Congress will point to a problem, and that is part of our job in terms of oversight and in terms of making sure taxpayers have their concerns responded to. But as we point fingers, we also ought to be constructive in terms of providing support. And sometimes that happens, and sometimes it does not.

But I noted in your testimony, Commissioner, on page 5—and I guess I am asking a question and answering it by reading this, but on the question of resources, you say, and I quote, "Congress can help by approving the President's fiscal year 2016 budget request, which includes $101 million specifically devoted to identity theft and refund fraud, plus $188 million for critical information technology infrastructure." So $101 million plus $188 million.

Can you tell us what those dollars would be used for?

Commissioner KOSKINEN. Yes. What they would do is, on the one hand, in terms of identity theft, they would improve our ability to more quickly upgrade our filter process. We have been building that for some time. We would go faster with that. It would allow us to, in fact, respond more specifically to individual taxpayers and their concerns. Most importantly, it would allow us to upgrade our basic IT infrastructure. As I noted earlier, we are running antiquated systems, some of which are no longer supported by the software companies.

And I would stress this particular problem was not a question of resources. My concern about it is, it is really a shot across the bow. The overall, ongoing challenge of dealing with sophisticated criminals around the world is the security of the entire system, and that is where the weaknesses in our antiquated system come to bear. So whatever resources we can have to continue to improve the overall system will be helpful.

Senator CASEY. And I hope if there is anything additional, either by way of authority or resources you need when it comes to dealing with the international dimensions to this, which I am sure are challenging, I hope you indicate that to us.

Thanks very much, Mr. Chairman.

The CHAIRMAN. Thank you, Senator.

Senator Heller, you are next.

Senator HELLER. Mr. Chairman, thank you. Thanks for holding this hearing. I also want to thank our witnesses for being here also.

Commissioner, I want to thank you for the call we had yesterday. It was very, very helpful, and hopefully we can move forward on some ideas. In fact, I will even bring them up, for that matter, as you probably anticipated. They will not be part of my questioning, but I think they are issues that are important to my home State.

I have heard from many of my constituents their strong concerns over the proposed IRS changes to the filing of information returns for reported winnings from bingo, keno, and slot machines. Due to the administrative burden proposed, 13,000 customers have signed a petition so that the reporting threshold for bingo, keno, and slot machines would not be reduced, and I too share their concerns about these proposed rules.

Across the U.S., the gaming industry supports 1.7 million jobs and about $240 billion in activity—no small sum. My staff has had multiple conversations with your office in regards to these proposed rules, and I am pleased that we had that opportunity to have the same discussion between you and me yesterday.

That said, I, like many other taxpayers, was frankly kept in the dark with regards to receiving responses from the IRS to better address these proposed rules. My questions were answered yesterday, some of them. I am grateful for that. Your comment period is extended, and I appreciate that, since it did take a couple months in order to get a response from your office. So, as I mentioned yesterday, my comments will be coming in the next week or so. Anyway, thank you for your help and support in extending the deadline in order to get those questions in.

The chairman talked a little bit about public trust for the IRS's success, and you are familiar with that. The number of weaknesses—the ability to effectively protect taxpayers' confidentiality, integrity, and availability of certain taxpayer data unfortunately was not implemented. The Inspector General is here. He spoke on it a little bit, and you alluded to it during your testimony.

It is my opinion, though, that a properly done tax reform would not only provide a simpler code, but would also provide the IRS with tools to combat tax-related identity theft and assist the victims of this crime.

I told you yesterday on the phone that I am here to help. How can I help you?

Commissioner KOSKINEN. Well, I appreciate that, and I appreciate, again, the chairman's clarity about how we need to work together on this. It is not a political issue. As we have said for some time, we need to get information returns earlier. It would be a great help to us. We need to have the authority to do what is called "mark" W–2s so that we can assure that they are produced by le-

gitimate companies, not by fraudulent companies, as we go forward.

We may need authority, to work with the partnership we have with the tax preparers and tax software companies as well as the States, to provide minimum requirements for data that authenticates taxpayers when they file their tax returns as we go forward.

And then, ultimately, as I have noted, our discussion today is not about something that was a result of a funding shortage, but the challenge we face more broadly dealing with the criminal enterprises around the world does depend upon making sure we have adequate funding to continue to rebuild our systems to get them into what I call "the early 21st century" rather than the late 19th century.

Senator HELLER. Yes. Commissioner, a previous Finance Committee Chairman, Max Baucus, had discussed a draft that would disallow taxpayer Social Security Numbers on W–2 forms. What is your view of this proposal? I would ask the same thing of the Inspector General.

Commissioner KOSKINEN. We have suggested that actually we just ought to get the last four digits on a W–2 form. What is more important to us is, if we can put so-called hashtags on those—and then we may need legislative authority—much like the number of companies that can provide paper that produces the money is allowed to be constrained by statute, we may need to be able to have those who produce W–2s through a competitive process be limited in number so that we can make sure that W–2s and the hashtags are appropriate as a way of, again, trying to make sure that the identifier is legitimate.

Senator HELLER. Okay. Mr. George, do you think that would be helpful?

Mr. GEORGE. I do, actually, Senator. I agree with the Commissioner there.

Senator HELLER. Okay. Mr. Chairman, my time has run out. Thank you.

The CHAIRMAN. Well, thank you, Senator.

Mr. George, let me just ask you an unrelated question while you are here. It is an important subject. For almost a year, at our request, TIGTA has been investigating Lois Lerner's hard drive crash. Last month, TIGTA gave the committee the last of the e-mails pulled from IRS backup tapes. As I understand it, the next and final step is for you to provide us with a report on your investigation, and now that all of the recovery work is done, can we get a commitment from you today to submit your report to us on the hard drive crash by mid-June?

Mr. GEORGE. I can commit, Mr. Chairman, to having it to you by the end of the month. I spoke with my chief investigator prior to this hearing in anticipation of the subject coming up. As of now, we have conducted over 100, almost 150 interviews of people related to the lost e-mails, and, as you can imagine, each interview leads to more information that needs to be tracked down.

Given the nature of this matter, we need to be as thorough as possible, and we are endeavoring to do just that. And I can say there are still very important interviews to come. So we will do our level best to try to accommodate that request, sir, but I can assure

you, you will have it before the end of the month, the Congress will.

The CHAIRMAN. Okay. Well, we will live with that. We would like to get our final report done, if we can.

Commissioner KOSKINEN. I would just like to go on the record saying I would be delighted to get everybody's final reports.

The CHAIRMAN. I am not sure that was helpful. [Laughter.] But we are glad you are glad, is all I can say.

Senator Roberts has a question or two. Then I would like to start the second round.

Senator ROBERTS. I would like to go back to that statement I inserted for the record. Nina Olson leads the Taxpayer Advocate Service, an independent office at the IRS. And in her annual report, she noted that victims must often navigate a labyrinth of IRS operations and recount their experience time and time again to different employees. Even when cases remain in one IRS function, they may be transferred from one assister to another with significant periods of non-activity. On average, the agency took nearly 6 months to resolve cases. She added that cases were also frequently closed prematurely before all related issues had been fully addressed. She recommended that a single officer be assigned to handle each case, and then she spoke to a broader issue, which I think really sums up what we are after here. While granting taxpayers enhanced access to their tax information, which was the laudable goal that even Congress agreed to when we passed this bill, the overriding priority now must be to protect taxpayers' confidential tax information from exposure. Is that a fair statement?

Commissioner KOSKINEN. I think, you know, as the Inspector General said and most people have said, it is a balancing act. As I say, we had 23 million successful downloads of the transcript. If those people had to call us or show up in person to get their transcript, it would have been a problem.

But, on the other hand, we need to make sure that we are as secure as possible. I think what is happening across the economy is that customers and taxpayers now understand that it may be harder to get access to their accounts, whether it is a bank account or—not harder in the sense it takes you 2 weeks, but there may be more hurdles you have to go through. You may have to have more information available to be able to get access. And I think taxpayers and customers are willing now and understand the need to accept the higher level of burden. And so we are reconsidering all of our work in that context in terms of where we go.

It should be noted that over 20 percent of the people who try to get their transcript downloaded cannot answer the questions, their own personal questions. But on the other hand, I think what this does remind us all is that, no matter how important it is to be providing excellent taxpayer service, we have to focus as much as we can on the security of the data, and that is a critical issue for us.

Senator ROBERTS. Mr. George, do you agree with that?

Mr. GEORGE. I do, Senator.

Senator ROBERTS. The IRS urged taxpayers not to contact the agency, the 104,000, saying it would only delay the already overburdened staff. Anyone whose information was stolen will be contacted. Sort of like "hurry up and wait."

Commissioner KOSKINEN. Well, they will not have to wait long. The letters are already——

Senator ROBERTS. Have letters been sent to all the 104,000?

Commissioner KOSKINEN. Yes—104,000 letters.

Senator ROBERTS. And what do the letters say that the person should do?

Commissioner KOSKINEN. They basically give instructions about how to get credit protection at our expense. They give them information about how to obtain an IP PIN if they would like one, the documentation they will have to provide. It gives them a number to call, but suggests that if they have question, they go to our website where we have provided a set of frequently asked questions about the situation and what can be done.

Senator ROBERTS. And you are confident you have the ability to protect this information with the suggestions you have in that letter?

Commissioner KOSKINEN. Yes. In fact, we advise them in that letter that we have marked their account so that no one else can file a return with their own information, and we——

Senator ROBERTS. I appreciate that. Thank you, Mr. Chairman.

The CHAIRMAN. Thank you.

Let me just ask—I apologize to you, Senator Carper. I should have called on you first.

Senator CARPER. Mr. Chairman, I have already had one bite out of the apple while you were out of the room, and I will wait my turn.

The CHAIRMAN. Okay. Well, let me just—Mr. George, in 2012 TIGTA did an audit of the IRS Computer Security Incident Response Center, or CSIRC, which is responsible for preventing and detecting computer security threats to IRS systems. In that 2012 audit, TIGTA found that the IRS was not monitoring 34 percent of its servers, and you noted that, "Without adequate monitoring of IRS servers, the CSIRC may not timely detect malicious activity or cyber-security incidents."

Could the IRS's failure to monitor its servers lead to the type of breach that occurred in May? That is question number one. And does TIGTA plan to reassess whether the CSIRC is now actively monitoring all IRS servers?

Mr. GEORGE. "Yes" is the answer to your first question, Mr. Chairman, and, yes, we will also be monitoring that.

The CHAIRMAN. Okay. Mr. George, the IRS is planning to expand the additional online services that it offers in the coming years. One notable example is the secure messaging pilot program that is scheduled to launch in 2016 that will allow the IRS to e-mail taxpayers and practitioners about sensitive tax information, something which the IRS has not done in the past, as I understand it.

In light of the recent data breach, do you have concerns about the security of online services that the IRS plans to introduce? And beyond current measures, what must the IRS do to ensure that these services are secure?

Mr. GEORGE. The IRS has sent the message in the wake of a lot of these attempts to gain access to taxpayers' identity or other information, and the message was, you know, "We never reach out to you by e-mail," and the like. And so they will have to engage

in a public service information effort, I think, to inform taxpayers about these new ways of approaching the system of tax administration.

Ultimately, it is a worthwhile goal to be able to contact people by way of e-mails and alternate ways of contacting them versus paper contact, which is much more expensive—and obviously so when you have individuals attempting to help taxpayers at Taxpayer Assistance Centers and the like. So it is a way for the IRS to more efficiently and effectively assist taxpayers to comply with their tax obligation. It is a good thing. There is no question that TIGTA will be looking at the overall proposal, how it is implemented, and the impact that it has on taxpayers.

The CHAIRMAN. Well, thank you. We appreciate the service that you render. It is a tough job, both of you.

Senator Heller, do you have any questions?

Senator HELLER. Mr. Chairman, thank you. I just have a couple of quick questions. I probably will not take all my 5 minutes, but these are issues that I think are important.

The last question I asked, Commissioner, was: How can we help? And I want you to explain to me why critical pay authority should be renewed.

Commissioner KOSKINEN. The streamlined critical pay authority has two aspects. The most important in many ways is the streamlined part, and primarily we use it for advanced-technology people. We can find somebody like the head of our Information Technology system, who worked at Boeing, and we can recruit them, and, much as in the private sector, if we find the right person, we can make them an offer, and they can accept it and start immediately.

The government process requires us to go through a complicated process that takes sometimes 3 to 4 months, and for the kind of people, the handful you are talking about recruiting, they often cannot wait 3 to 4 months or will not wait 3 to 4 months. Our IT head told me we have two people we have tried to hire in the IT department who, if we had streamlined critical pay, would have come. They did not want to participate in a 3- to 5-month process and, therefore, turned us down.

Senator HELLER. The authority expired in 2013.

Commissioner KOSKINEN. Correct.

Senator HELLER. What has been the impact between then and today, outside the story you just told me?

Commissioner KOSKINEN. Well, we have had 29 people on streamlined critical pay authority. We were authorized no more than 40, and we never used more than 34 of them, so we did not just put people in. We are down now to 15 or 16. We have lost our Senior International Expert in Tax Enforcement. We have lost the Deputy CIO. We have lost the three people who are best at big data analysis, including our expert on authentication. Their term ran out, and we have not been able to replace them.

Senator HELLER. One follow-up. I do not have to tell you about your budget. You know your budget a lot better than I do. But in 2014, it is my understanding you spent in the area of $2.4 billion or 21 percent of your budget in information technology. With that budget being that substantial, do you have the experts that you need in cyber-security?

Commissioner KOSKINEN. We at this point have the experts. In fact, a key executive in cyber-security is on streamlined critical pay. He will rotate off.

Senator HELLER. Okay. That was my next question.

Commissioner KOSKINEN. If we do not have the possibility, we will not be able to get them in. Of the budget in 2014, about 80 percent of it goes to simply operating and maintaining our system, so that our challenge in 2014 was, for instance, we asked for $300 million in IT to implement the Affordable Care Act. We got zero. So we had to take $300 million out of other IT programs, and the same thing happened in 2015.

Senator HELLER. Do you feel you have well-qualified hires?

Commissioner KOSKINEN. We have a spectacular workforce. It is the best workforce I have ever dealt with, and I have dealt with a lot of different enterprises in the private sector for 20 years and in the government. It is a dedicated workforce. Even with all the pressure and sometimes the abuse they take, they are dedicated to the mission, and the mission is based on helping taxpayers.

Senator HELLER. Okay. Commissioner, thank you.

Mr. Chairman, thank you.

The CHAIRMAN. My understanding is that Senator Carper would like to ask a couple of questions, but first I would like to thank both of you for being here, and I appreciate the testimony you have given here today.

Mr. Koskinen, you have a tough job. There is no question about it. I do not know anybody who approaches it with a smile like you do, and I would be upset every day. And I think there is something wrong with you that you are not upset every day. [Laughter.]

On the other hand, I know you are.

And, Mr. George, we are very pleased with the hard work that you do—and your group down there. It is important that we have both of you working in the best interests of our country and of our taxpayers, and I really have appreciated you over the time that I have known you and the time you have been advising the committee.

Mr. GEORGE. Thank you, Senator.

The CHAIRMAN. With that, we will turn to Senator Carper, and hopefully finish up with Senator Carper.

Senator CARPER. Thanks, Mr. Chairman.

I am an old State treasurer and an old Governor, and I have been thinking about these attacks on the IRS. And, as you know, there are 50 States. They all have their own divisions of revenue. Has anyone given any thought to how to better help them prepare to defend information and defend their treasuries from attacks like this? Is there any discussion of that?

Commissioner KOSKINEN. As I say, we have had and now have a much more formal partnership and working relationship with States, with tax administrators. We are sharing information. We are trying to provide them as much assistance as we can about what we know. As I say, this is no longer the problem of any individual organization. This is a systemic challenge across the entire economy. There is a website somebody sent me that had the indications that of the 25 cyber-attacks and data breaches in May alone, 25 around the world, we are just one of those 25.

So we take it seriously. We need to deal with it aggressively. But we need to understand, it is in the context of a significant systemic set of attacks.

Senator CARPER. I think I heard you say, Commissioner Koskinen, describing the information that was included in the letters going out, I thought I heard you say the term "IP PIN" in one of your answers. Would you just elaborate on that, please?

Commissioner KOSKINEN. Yes. An Identity Protection PIN is a separate 6-digit number that is given to taxpayers if they are the victims of identity theft which they use to file in addition to their Social Security Numbers. They will have their Social Security Number, because we can check that against W–2s. But on the 1040 there is a point where they will include their IP PIN. If the IP PIN does not appear, the return is not accepted. So it protects them against anyone filing a fraudulent return with their Social Security Number alone.

Senator CARPER. All right. Thank you. I know it is still early in the review process, but do you intend to reinstate the Get Transcript online application? And if so, how do you balance the need for additional security against the need for taxpayers to have a convenient means of gathering access to old returns?

Commissioner KOSKINEN. Well, it is the conundrum we face in any of these applications. As I say, we had 23 million successful downloads. That is a lot of taxpayer service. We will not put it back up unless we are satisfied that the security is, in fact, appropriate. It does mean that it is going to be more difficult for taxpayers, and more of them will not be able to get through. Already some of them cannot get through the existing security measures. But again, I think taxpayers are in a position to understand that.

We are looking at the lessons learned from this event. We are delving into at great length exactly how it happened, what could be done in the security issues to make it more difficult for it to happen, if not impossible. But as you know, it is a continual tradeoff of trying to provide as much information as readily to taxpayers as we can, but at the same time protecting that data.

Senator CARPER. We have heard a fair amount today about upgrading the IRS's IT systems. Will the President's fiscal year budget request be sufficient, if it is met, to meet those needs? Or is that request from the President, from the administration, for 2016 just the beginning of a multiyear effort to upgrade your computer systems?

Commissioner KOSKINEN. The President's budget would allow us to, in fact, make significant progress in 2016, but your point is well taken. We have been working on upgrading the system for some time. We are not going to be able to do it in 1 year. One of the things we are working on with the appropriators is to give them a longer-term view of what it actually takes both to upgrade the systems and also to provide secure, increased availability of information to taxpayers.

Senator CARPER. All right. We talked a moment ago about partnership and reaching out to the States and making sure that they learn from us at the Federal level, and maybe we can learn a few things from them to provide better protection against these attacks. Are there any other countries that we are communicating with that

have thought through these problems and responded to these same kinds of challenges that we may be able to glean some helpful ideas from?

Commissioner KOSKINEN. We are in contact—I belong to a group of the 43, in effect, largest tax administrators around the world. We seem, primarily because, I think, of the size of the economy and the attractiveness of it, to have more of these challenges than others. But security is on all of their minds. Those with a value-added tax have less concern about individual taxpayers, as noted in the earlier discussion. But we are sharing information particularly with the OECD countries. But as I say, thus far in the meetings I have had with them, we seem to be having more challenges as an economy as well as a tax administration system.

Senator CARPER. And a last question, if I could, Mr. Chairman, maybe of Inspector General George. A year or so ago a firm, I want to say it might have been—I am not sure of the name of the firm—but a U.S. firm that specializes in protection against cyber-attacks, a private firm—Mandiant. I think it was Mandiant. Someone did a fair amount of work on attacks emanating from China, and they actually drilled down and said, "These are the folks, this is where they are located, these are the people who are actually launching these attacks against our country." The Chinese did not accept it very well, but I have not seen anything to refute the veracity of the assertions.

I always like to focus on root causes. I like to focus on root causes, and I keep trying to figure out how do we go on a root-cause approach to deal with this issue, but it is just spreading. In our own family, we have been involved in a hack against the university that we are associated with, with our health care provider, now in this case with the issue at hand. So I like to say, the third time is the charm, I hope. I hope it is over. But my guess is it is not for us. But how do we go about the root cause of getting to this? Again, is there some way—everybody keeps saying it is coming from Russia, Russian criminal organizations. Is there not anything we can do about that?

Mr. GEORGE. Well, if it is addressed to me, sir, I mean, Willie Sutton said, "That is where the money is." And of course, having the world's largest economy, as the Commissioner suggested, you know, it attracts the bad guys.

While I am not familiar with the study you just cited citing China as the source of a lot of these problems, on a number of the criminal investigations that have been completed by us, a lot of them did emanate from former Soviet republics—Belarus and places like that. It is again, sir, just too many people who have too much time on their hands, and with their sophistication that relates to computers and networks and servers and the like, it is truly a challenge, and not just for the Internal Revenue Service. As has been stated before, both by the Commissioner and members of this panel, this is a Federal, State, local, global problem. And I do not see it ending any time soon, sir, because, just as soon as the IRS increases its security posture, the bad guys will increase their efforts to overcome those, and they have a lot of time on their hands.

Senator CARPER. Mr. Chairman, I would just say in closing, we spend a lot of time trying to focus on the symptoms of problems in all kinds of ways. We do not always focus on the root causes. And one of the things that it is important that we focus on is the symptoms and defending against these attacks in ways that have been discussed here today. But at the same time, we need to be thinking about root causes as well. And I am not sure how to do that, but we need to think about that.

Thank you so much, and thanks to our witnesses.

The CHAIRMAN. Thank you, Senator Carper.

Senator Nelson?

Senator NELSON. Mr. Chairman, these are numbers of confirmed tax-related identity theft victims: Florida, 334,962; Utah, 10,654; Delaware, 4,703. Senator Carper, you had 4,703 of your constituency who were victims of identity theft. Total U.S., D.C.: 1,889,736. If you include the U.S. territories and unconfirmed residents, we are talking about 2.75 million.

Now, Mr. Chairman, we have had six hearings on identity theft, and yet we continue to bring in the IRS. We ought to take care of this by passing legislation. I filed legislation, you filed legislation. Your legislation has a lot of similarities with our legislation. We ought to get something moving.

The CHAIRMAN. Let us get together and get it done. I agree with you.

Senator NELSON. Excellent.

The CHAIRMAN. All right.

Senator NELSON. So put on the record, Mr. Commissioner, what tool would help you on this, which I think is in the legislation, but I suspect you want to get that out there on the record.

Commissioner KOSKINEN. Yes. As we said earlier in the hearing, the legislation we have increasing support on the Hill for—we need to get information returns, particularly W–2s, earlier. We need to get them in January when employees get them so that we can, in fact, before we send out refunds, have a better chance of checking the return data.

We also need to have authority to, in effect, use what are called hashtags with industry on those W–2s to make sure that the W–2s themselves are accurate. Criminals are now forming false corporations and generating false W–2s to go along with their fraudulent returns.

We need to provide minimum standards for qualifications for education for tax preparers, which you have talked about in your bill. We need to increase the penalties for engaging in identity theft and refund fraud. Those are requests in our budget proposal. They are in your legislation. We are delighted to work with you and with the chairman to put together a final package that would give us additional tools.

I would stress they will be important and very helpful, but as the Inspector General and I have both been saying, there is no magic silver bullet that tomorrow morning is going to put this all to an end. We need to continue to be vigilant. We will need to continue to do everything we can with our systems, with our security, with our monitoring of it. But clearly, the items that are contained in

the legislative discussions you and the chairman have been having are going to be important.

Senator NELSON. Okay. That is my point, Mr. Chairman, and——

The CHAIRMAN. Still, let us get together.

Senator NELSON. Let us do it. And, Mr. Chairman, I became alerted to this—this is what is shocking. This was about 4 years ago. Street crime in Tampa, FL dropped—burglaries, auto thefts, muggings dropped—because the criminals suddenly realized: get a laptop, go in and create a false return, and get a refund. And it was all of a sudden too easy to get money.

Now, it is a good thing that people's homes were not being burglarized, but nevertheless, people were being robbed. In this case, it is not only individuals who had a nightmare, by the way—and thanks to the IRS; you have helped us administratively once a taxpayer has a false return in their name—but then all of the other ID trauma that they go through getting back their ID. But it suddenly had a whole shift, and the taxpayers are paying because of this theft.

So thank you, Mr. Chairman.

The CHAIRMAN. Thank you, Senator.

I want to thank Commissioner Koskinen and Inspector General George for appearing before the committee today, as well as all of the Senators who have participated. This has been a very interesting hearing for me.

Commissioner Koskinen, three unrelated but important points before we wrap up.

First, in recent months I have written to you regarding the reissuance of the proposed rule on political activity by tax-exempt organizations. You know how interested this committee is in this matter. Can you tell me when the IRS and Treasury Department will reissue the proposal?

Commissioner KOSKINEN. If I had a crystal ball, I would be better at giving you that information. We have spent a lot of time, we had 160,000 responses we took very seriously. I personally have read over 1,200 pages of thoughtful responses. We are moving forward. My commitment has been that——

The CHAIRMAN. Keep me informed.

Commissioner KOSKINEN. Yes. My commitment has been that we will keep you informed. You will not be surprised. We will keep you updated before we actually issue a proposal, and it will provide for 90 days of comment and a subsequent public hearing. So we do not want anybody to think we are rushing this. We are only going to do this once. We are not going to do it every 2 or 3 years.

The CHAIRMAN. Well, I want to end that chapter of mistreatment of conservative groups—liberal groups. I do not care. It just should not happen, and I am counting on you to straighten it out.

Commissioner KOSKINEN. Yes. As I have said, we want to have a rule that is clear, fair to everybody, easy to administer, and easy to operate a (c)(4) organization under so you do not have to worry about somebody second-guessing you in the future.

The CHAIRMAN. That would be great.

Second, in April, I wrote to Secretary Lew requesting documents relating to the 2013 political activity rule. He has declined that request, and I will be responding to him on the matter.

Now, I wanted to give you notice that I will be sending a similar request to your agency, and I look forward to working with you on that in the near future.

Finally, in April, I wrote to you regarding the IRS's spending on information technology, and I want to thank you for acknowledging my letter, and I look forward to receiving a thorough response as soon as possible, if you can.

Commissioner KOSKINEN. It is a lot of data to pull together, but I think it will be very helpful because it does answer a range of very detailed questions about priorities, about our experience, how we monitor it all, and, with a little luck, we will get it to you very quickly.

The CHAIRMAN. Well, thank you. I hope you are very lucky. I want to thank both of you very much. This has meant a lot that you would come up on such short notice.

Any questions for the record should be submitted by no later than Tuesday, June 9th.

With that, the hearing is adjourned.

[Whereupon, at 11:56 a.m., the committee was adjourned.]

APPENDIX

ADDITIONAL MATERIAL SUBMITTED FOR THE RECORD

PREPARED STATEMENT OF HON. J. RUSSELL GEORGE, TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION, DEPARTMENT OF THE TREASURY

Chairman Hatch, Ranking Member Wyden, and Members of the Committee, thank you for the opportunity to testify on the data breach that occurred at the Internal Revenue Service (IRS).

The Treasury Inspector General for Tax Administration, also known as "TIGTA," is statutorily mandated to provide independent audit and investigative services necessary to improve the economy, efficiency, and effectiveness of the IRS. TIGTA's oversight activities are designed to identify high-risk systemic inefficiencies in IRS operations and to investigate exploited weaknesses in tax administration. TIGTA's role is critical in that we provide the American taxpayer with assurance that the approximately 91,000[1] IRS employees, who collected over $3.1 trillion in tax revenue, processed over 242 million tax returns and other forms, and issued $374 billion in tax refunds[2] during Fiscal Year 2014, perform their duties in an effective and efficient manner while minimizing the risks of waste, fraud, or abuse. This includes investigating individuals who use the IRS as a means of furthering fraudulent, criminal activity that negatively impacts the operations of the IRS, as well as investigating allegations of serious misconduct by IRS employees and threats of violence against the IRS, its employees, and facilities. Over the past year, a significant part of our workload has been devoted to investigating scams that can negatively impact the integrity of tax administration.

OVERVIEW OF THE RECENT IRS DATA BREACH

On May 26, 2015, the IRS announced that criminals had used taxpayer-specific data acquired from non-IRS sources to gain unauthorized access to information onapproximately 100,000 tax accounts through the IRS's Get Transcript application.[3] TIGTA's Office of Investigations continues to investigate this incident, coordinating with other Federal law enforcement agencies. We ask for patience while we gather the evidence we need to determine who is responsible for this intrusion so they can be brought to justice. In addition, the evidence we are gathering is also critically important for us to understand the impact on the victims as well as to document exactly how this happened so it can be prevented in the future.

According to reports we received from the IRS, which we have not yet validated, an individual or individuals succeeded in clearing an authentication process that required knowledge of information about the taxpayer, including Social Security information, date of birth, tax filing status, and street address. In addition, it appears that these third-parties had access to private personal information that allowed them to correctly answer questions which typically only the taxpayer would know. This type of information can be purchased from illicit sources or fee-based databases, or obtained from social media sites.

The proliferation of data breaches reported in recent years and the types of information available on the Internet has resulted in a degradation of controls used to

[1] Total IRS staffing as of January 24, 2015. Included in the total are approximately 19,000 seasonal and part-time employees.
[2] IRS, *Management's Discussion and Analysis, Fiscal Year 2014,* page 2.
[3] Information available on the Get Transcript application can include account transactions, line-by-line tax return information, and income reported to the IRS.

authenticate individuals accessing personal data in some systems. The expansion of e-commerce services often conflicts with the tenets of strict security standards. Providing taxpayers more avenues to obtain answers to their tax questions or to access their own tax records online also creates greater risk to an organization and provides more opportunities for exploitation by hackers and other fraudsters.

In its most recent Strategic Plan,[4] the IRS acknowledged that the current technology environment has raised taxpayers' expectations for online customer service interactions and it needs to meet these expectations. However, the risk for this type of unauthorized access to tax accounts will continue to grow as the IRS focuses its efforts on delivering taxpayers self-assisted interactive online tools. The Commissioner of Internal Revenue's vision is to provide taxpayers and tax professionals with electronic products and services that they desire to enable them to interact and communicate with the IRS. This includes more robust online services, based on the idea of accessing Government services anywhere, any time, on any device, in three to 5 years. For example, the IRS is acquiring software and contractor services for a Secure Messaging Pilot Program to be launched in Fiscal Year 2016 that will lay the foundation for a broader taxpayer digital communication rollout in the future.

In addition to the IRS's Get Transcript application, the IRS also requires taxpayers to authenticate their identities for certain other services on its public Internet site or its toll-free customer service lines, which could also pose a risk for unauthorized access. In June 2014, the IRS established its Authentication Group to provide oversight and facilitate the development and implementation of authentication policies and processes across the IRS's business functions. Due to the significant risks in this area, we currently have an audit underway to assess the IRS's processes for authenticating taxpayers at the time tax returns are processed and when accessing IRS services.[5]

DATA SECURITY REMAINS A TOP CONCERN OF TIGTA

Since Fiscal Year 2011, TIGTA has designated the security of taxpayer data as the top concern facing the IRS based on the increased number and sophistication of threats to taxpayer information and the need for the IRS to better protect taxpayer data and improve its enterprise security program. In addition, the IRS has declared its Information Security program as a "significant deficiency" from a financial reporting standpoint, which means weaknesses in its internal control environment are important enough to merit the attention of those charged with IRS governance.

To provide oversight of the IRS's Information Security program, TIGTA completes approximately seven audits each year on various security programs, systems, and solutions. As of March 2015, these audits have resulted in 44 recommendations that have yet to be implemented. While most of these recommendations are based on recent audits, there are 10 recommendations from five audits that are over three years old. In addition, the IRS has disagreed with 10 of 109 recommendations from 19 audits relating to security that we performed during the period of Fiscal Year 2012 through Fiscal Year 2014.

We have identified a number of areas in which the IRS could better protect taxpayer data and improve its overall security posture. Most recently, we found two areas that did not meet the level of performance specified by the Office of Management and Budget and the Department of Homeland Security: (1) Identity and Access Management, and (2) Configuration Management.[6]

Identity and Access Management ensures that only those with a business need are able to obtain access to IRS systems and data. However, we found that the IRS needs to fully implement unique user identification and authentication that complies with Department of Homeland Security directives, ensure that users are only granted access based on needs, ensure that user accounts are terminated when no longer required, and control the improper use of shared accounts.

Configuration Management ensures that settings on IRS systems are maintained in an organized, secure, and approved manner, including timely updating patches to known security vulnerabilities. We found that the IRS needs to improve enter-

[4] *Internal Revenue Service Strategic Plan—FY 2014–2017* (IRS Publication 3744), pgs. 6–7 (June 2014).

[5] TIGTA, Audit No. 201440016, *Efforts to Authenticate Individual Income Tax Return Filers Before Tax Returns Are Processed,* report planned for August 2015.

[6] TIGTA, Ref. No. 2014–20–090, *Treasury Inspector General for Tax Administration—Federal Information Security Management Act Report for Fiscal Year 2014* (Sept. 2014).

prise-wide processes for assessing configuration settings and vulnerabilities by means of automated scanning, timely remediating scan result deviations, timely installing software patches, and controlling changes to hardware and software configurations.

Patch [7] management is an important element in mitigating the security risks associated with known vulnerabilities to computer systems. This is critical to prevent intrusions by unauthorized individuals or entities. Due to its importance, TIGTA evaluated the effectiveness of the IRS security patch management process, which has been an ongoing challenge for the IRS.[8] We found that the IRS has made progress in automating installation and monitoring in a large segment of its computers, but it has not yet implemented key patch management policies and procedures needed to ensure that all IRS systems are patched timely and operating securely. Any significant delays in patching software with critical vulnerabilities provides ample opportunity for persistent attackers to gain control over vulnerable computers and get access to the sensitive data the computer systems may contain, including taxpayer data.

We have also identified other areas that would improve the IRS's ability to defend its systems against cyber-attacks. Monitoring IRS networks 24 hours a day yearround for cyber-attacks and responding to various computer security incidents is the responsibility of the IRS's Computer Security Incident Response Center (CSIRC). TIGTA evaluated the effectiveness of the CSIRC at preventing, detecting, reporting, and responding to computer security incidents targeting IRS computers and data.[9] We found that the CSIRC is effectively performing most of its responsibilities for preventing, detecting, and responding to computer security incidents. However, further improvements could be made. At the time of our review, the CSIRC's host-based intrusion detection system was not monitoring a significant percentage of IRS servers, which leaves that portion of the IRS network and data at risk. In addition, the CSIRC was not reporting all computer security incidents to the Department of the Treasury, as required. Finally, incident response policies, plans, and procedures were either nonexistent, inaccurate, or incomplete.

One of the Federal Government's latest security initiatives is the implementation of information security continuous monitoring, which is defined as maintaining ongoing, real-time awareness of information security, vulnerabilities, and threats to support organizational risk decisions. While the IRS has made progress and is in compliance with Department of Homeland Security and Department of the Treasury guidelines, we have found that, based on the large scale of the IRS's computer environment, a one-size-fits-all approach does not provide the best security for the IRS.[10]

We have also previously raised concerns over the remediation of security weaknesses identified in our audits. Management controls are a major part of managing an organization and provide reasonable assurance that organizational objectives are achieved. We have reviewed closed corrective actions to security weaknesses and findings reported by TIGTA and identified weak management controls in the IRS over its closed planned corrective actions for the security of systems involving taxpayer data.[11] During our audit, TIGTA determined that eight (42 percent) of 19 planned corrective actions that were approved and closed by the IRS as fully implemented in response to reported security weaknesses from prior TIGTA audits were only partially implemented.

Management control also involves the use of risk-based decisions by IRS management to make an exception to its own policies and requirements based on suitable justification and a thorough assessment of evident and potential risks. For decisions related to the security of information systems, exceptions are allowed if meeting the requirement is: (1) not technically or operationally possible, or (2) not cost effective.

---

[7] A patch is a fix of a design flaw in a computer program. Patches must be installed or applied to the appropriate computer for the flaw to be corrected.

[8] TIGTA, Ref. No. 2012–20–112, *An Enterprise Approach Is Needed to Address the Security Risk of Unpatched Computers* (Sept. 2012).

[9] TIGTA, Ref. No. 2012–20–019, *The Computer Security Incident Response Center Is Effectively Performing Most of Its Responsibilities, but Further Improvements Are Needed* (Mar. 2012).

[10] TIGTA, Ref. No. 2014–20–083, *The Internal Revenue Service Should Implement an Efficient Internal Information Security Continuous Monitoring Program That Meets Its Security Needs* (Sept. 2014).

[11] TIGTA, Ref. No. 2013–20–117, *Improved Controls Are Needed to Ensure That All Planned Corrective Actions for Security Weaknesses Are Fully Implemented to Protect Taxpayer Data* (Sept. 2013).

We found that these risk-based decisions were not adequately tracked and documented. Without required supporting documentation, we could not determine why decisions were made and whether the information technology risks were appropriately accepted and approved.[12]

ATTEMPTS TO DEFRAUD TAX ADMINISTRATION ARE INCREASING

Due to its mission, the trillions of dollars that flow through the IRS each year, and the hundreds of millions of taxpayer data sets used and maintained by the IRS, the IRS is continuously under attack by criminals using the tax administration system for personal gain in various ways. These scams, and the methods used to perpetrate them, are constantly changing and require constant monitoring by the IRS. For at least the last decade, the IRS has provided the public with information about what it sees as the "Dirty Dozen" tax scams on its website. These scams range from offshore tax avoidance to fake charities, and inflated refund claims. Compiled annually, the "Dirty Dozen" lists a variety of common scams that taxpayers may encounter.

In addition to the data breach discussed previously, two of the most pervasive frauds currently being perpetrated that impact tax administration are the phone impersonation scheme and identity theft.

Phone Impersonation Scam

The phone impersonation scam has proven to be so large that it is one of TIGTA's Office of Investigation's top priorities, and it has also landed at the top of the IRS's "Dirty Dozen" tax scams this year. It has proven to be a surprisingly effective and fast way to steal taxpayers' money, and in this fast-paced electronic environment, the money can be gone before the victims ever realize that they have been scammed. The number of complaints we have received about this scam makes it the largest, most pervasive impersonation scam in the history of our agency. It has claimed thousands of victims with reported losses totaling almost $19 million to date.

We first started seeing concentrated reporting of these calls in August 2013. As the reporting continued through the fall, in October 2013 we started to specifically track this crime. To date, we have received hundreds of thousands of complaints about these calls. According to the victims, the scam artists made threatening statements and then demanded that the victims immediately put money on prepaid debit cards in order to avoid being arrested. The callers often warned the victims that if they hung up, local police would come to their homes to arrest them. The scammers may also send bogus IRS e-mails to support their scam. Those who fell for the scam withdrew thousands of dollars from their bank accounts and then purchased the prepaid debit cards as instructed by the callers. Once the prepaid debit cards were purchased, the perpetrators instructed the victims to call them back and read them the numbers on the prepaid card. By the time the victims realized they had been scammed, the perpetrators had negotiated the prepaid cards and the money was gone.

To date, TIGTA has received over 525,000 reports of these calls. We continue to receive between 9,000 and 12,000 reports of these calls each week. As of May 25, 2015, 3,700 individuals have been victimized by this scam and have paid a total of almost $19 million, an average of approximately $5,100 per victim. The highest reported loss by one individual was over $500,000. In addition, 296 of these victims also provided sensitive identity information to these scammers.

The perpetrators do not discriminate; they are calling people everywhere, of all income levels and backgrounds. Based on a review of the complaints we have received, we believe the calls are now being placed from more than one source. This scam is the subject of an ongoing multi-agency investigation. There is much that we are doing to apprehend the perpetrators, but TIGTA is not at liberty to disclose specifically what is being done as it may impede our ability to successfully bring these criminals to justice. I can tell you that it is a matter of high priority for law enforcement.

However, there is much more that needs to be done, as these examples are part of a broader ring of scam artists operating beyond our borders. This is unfortunately similar to most of the cyber-crime we are seeing today—it is international in nature and committed by means of technology (*e.g.,* in the case of the phone fraud scam, the use of Voice over Internet Protocol technology), and much of it originates from

[12] TIGTA, Ref. No. 2014–20–092, *The Internal Revenue Service Does Not Adequately Manage Information Technology Security Risk-Based Decisions* (Sept. 2014).

computers outside the United States. To further deceive their intended victims, by using this technology, the criminals create false telephone numbers that show up on the victim's caller ID system. For example, the criminals make it appear as though the calls are originating from Washington, DC or elsewhere in the United States.

Identity Theft

Another challenging area impacting tax administration is the growth in identity theft. At the same time the IRS is operating with a reduced budget, it continues to dedicate significant resources to detect and review potential identity theft tax returns as well as to assist victims. Resources have not been sufficient for the IRS to work identity theft cases dealing with refund fraud, which continues to be a concern. A critical component of preventing and combating identity theft refund fraud is the authentication of a taxpayer's identity at the time tax returns are processed.

During the past several years, the IRS has continued to take steps to more effectively detect and prevent the issuance of fraudulent refunds resulting from identity theft tax return filings. The IRS reported that in Filing Season 2013, its efforts prevented between $22 billion and $24 billion in identity theft tax refunds from being issued.[13] This is a result of the IRS's continued enhancement of filters used to detect tax returns that have a high likelihood of involving identity theft at the time the returns are processed. For example, the IRS used 11 filters in Processing Year (PY) 2012 to identify tax returns with a high likelihood of involving identity theft, compared to the 114 filters it used in PY 2014. The use of these filters assists the IRS in more effectively allocating its resources to address identity theft tax refund fraud.

The IRS has also taken steps to more effectively prevent the filing of identity theft tax returns by locking the tax accounts of deceased individuals to prevent others from filing a tax return using their names and Social Security Numbers. The IRS has locked approximately 26.3 million taxpayer accounts between January 2011 and December 31, 2014. In addition, the IRS issues an Identity Protection Personal Identification Number (IP PIN) to any taxpayer who is a confirmed victim of identity theft or who has reported to the IRS that he or she could be at risk of identity theft. However, we reported that the IRS did not provide an IP PIN to 557,265 eligible taxpayers for Processing Year 2013.[14] Once the IRS confirms the identity of a victim or "at-risk" taxpayer, the IRS will issue the taxpayer an IP PIN for use by the taxpayer when filing his or her tax return. The presence of a valid IP PIN on the tax return tells the IRS that the rightful taxpayer filed the tax return, thus reducing the need for the IRS to screen the tax return for potential identity theft. The IRS has issued more than 1.5 million IP PINs for PY 2015.

Despite these improvements, the IRS recognizes that new identity theft patterns are constantly evolving and that consequently, it needs to adapt its detection and prevention processes. The IRS's own analysis estimates that identity thieves were successful in receiving over $5 billion in fraudulent tax refunds in Filing Season 2013.

In summary, the IRS faces the daunting task of protecting its data and IT environment from the ever-changing and rapidly-evolving hacker world. This incident provides a stark reminder that even security controls that may have been adequate in the past can be overcome by hackers, who are anonymous, persistent, and have access to vast amounts of personal data and knowledge. The IRS needs to be even more vigilant in protecting the confidentiality of sensitive taxpayer information. Otherwise, as shown by this incident, taxpayers can be exposed to the loss of privacy and to financial damages resulting from identity theft or other financial crimes.

We at TIGTA are committed to our mission of ensuring an effective and efficient tax administration system and preventing, detecting, and deterring waste, fraud, and abuse. As such, we plan to provide continuing audit and investigative coverage of the IRS's efforts to effectively protect sensitive taxpayer data and investigate any instances of attempts to corrupt or otherwise interfere with tax administration.

Chairman Hatch, Ranking Member Wyden, and members of the committee, thank you for the opportunity to share my view.

---

[13] IRS Identity Theft Taxonomy, dated September 15, 2014, page 1.

[14] TIGTA, Ref. No. 2014–40–086, *Identity Protection Personal Identification Numbers Are Not Provided to All Eligible Taxpayers* (Sept. 2014).

QUESTIONS SUBMITTED FOR THE RECORD TO HON. J. RUSSELL GEORGE

QUESTION SUBMITTED BY HON. MARK R. WARNER

Question. It is my understanding that third-party vendors have signed up with the IRS to access taxpayer transcripts via the Income Verification Express Service. What is the IRS doing to ensure that these third-party vendors that have signed up with the IRS to access taxpayer transcripts have appropriate safeguards in place and are not vulnerable to data breaches?

Answer. In January 2011, we evaluated regulations and Income Verification Express Service (IVES) enrollment policies to ensure lenders, such as banks, and companies that specialize in making third-party requests for lenders (Income Verification Specialists) properly protect taxpayers' tax return information.[1] At that time, we determined that the IRS did not have a screening process and did not define minimum requirements in the form of a user agreement to help ensure IVES Program participants meet minimum standards and protect tax return information. In addition, we found the IRS did not require IVES Program participants to maintain electronic security and not disclose the information they receive from the IRS to nonaffiliated third parties.

We recently performed a review to determine if the IVES and Return and Income Verification Services programs had adequate processes and procedures in place designed to prevent inadvertent disclosures of taxpayer information.[2] The scope of this review was limited to the environment and processes under the IRS's direct control. We found that generally the appropriate controls were in place and that for Fiscal Years 2009 through 2013 approximately 118 million requests were processed and fewer than 800 inadvertent disclosure incidents were recorded. Our report recommendations related to how quickly disclosures should be reported, determining the method to document and fully report disclosures, ensuring quality review teams conduct all established tests, and ensuring that internal policies are properly updated to document the correct process for reporting inadvertent disclosures.

On June 1, 2016, we became aware of a fraud scheme in which perpetrators obtained sensitive tax and other identifying information and are using that information to order tax transcripts using the Transcript Delivery System (TDS). We have initiated a review to evaluate this issue as well as the adequacy of TDS's processes and procedures to ensure only authorized users obtain access to taxpayer information.[3]

QUESTIONS SUBMITTED BY HON. JOHN THUNE

Question. I understand that based on TIGTA's audit of tax year 2012, you reported that there were 787,000 fraudulent tax returns that went undetected by the IRS. This is actually an improvement, down from 1.1 million years for tax year 2011. How would you assess the progress being made by the IRS in preventing identity-theft related tax fraud? What overall grade would you give the IRS in this area?

Answer. The IRS continues to make significant improvements in its identification of identity theft tax returns at the time the returns are processed and before fraudulent tax refunds are released. For example, the IRS reports that in the 2013 Filing Season,[4] it detected approximately $24.3 billion in identity theft refund fraud. However, the IRS also recognizes that new identity theft patterns are constantly evolving and, as such, it needs to continue to adapt its detection and prevention processes. Consequently, the IRS continues to expand its filters used to detect identity theft refund fraud at the time tax returns are processed.

For example, the IRS used 11 filters in Processing Year 2012 to detect approximately 325,000 tax returns that prevented the issuance of approximately $2.2 bil-

---

[1] TIGTA, Ref. No. 2011–40–014, *The Income Verification Express Services Program Needs Improvements to Better Protect Tax Return Information* (Jan. 2011).

[2] TIGTA, Ref. No. 2015–IE–R004, *Requests for Taxpayer Information Were Generally Processed Properly in the Return and Income Verification Services and the Income Verification Express Service Programs* (Mar. 2015).

[3] TIGTA, Audit No. 201640032, *Review of the Transcript Delivery System,* report planned for June 2017.

[4] The period from January through mid-April when most individual income tax returns are filed.

lion in fraudulent tax refunds. In Processing Year[5] 2014 as of September 30, 2014, the IRS increased its filters to 114 and detected 832,412 tax returns, preventing the issuance of approximately $5.5 billion in fraudulent tax refunds. According to the IRS, for Processing Year 2015, it has increased the number of filters to 196 and detected 306,708 tax returns, preventing the issuance of about $2.2 billion in fraudulent tax refunds as of May 31st, 2015.

In addition, the IRS continues to expand the locking of tax accounts, which results in the rejection of an electronically filed (e-filed) tax return (*i.e.,* the IRS will not accept the tax return for processing). A locked tax account also prevents paper-filed tax returns from posting to the Master File if the Social Security Number associated with the locked tax account is used to file a tax return. Between January 2011 and May 31, 2015, the IRS locked approximately 28.6 million taxpayer accounts of deceased individuals. For Processing Year 2015 as of May 31, 2015, the IRS stopped 18,996 processed tax returns with refunds totaling approximately $31.4 million from posting to the Master File using the account locks. Additionally, the IRS has rejected (*i.e.,* did not accept for processing) 85,811 e-filed tax returns through the use of these locks.

For the 2013 Filing Season, the IRS also developed and implemented a clustering filter tool in response to TIGTA's continued identification of large volumes of undetected potentially fraudulent tax returns for which tax refunds had been issued to the same address or deposited into the same bank account. Tax returns identified are withheld from processing until the IRS can verify the taxpayer's identity. For Filing Season 2015 as of May 2, 2015, the IRS reports that, using this tool, it has identified 201,373 tax returns and prevented the issuance of approximately $496.5 million in fraudulent tax refunds.

Despite the improvements in identification of identity theft tax returns at the time the returns are processed and before fraudulent tax refunds are released, the IRS still does not have timely access to third-party income and withholding information. Most third-party income and withholding information is not received by the IRS until well after tax return filing begins. For example, the deadline for filing most information returns with the IRS is March 31st, yet taxpayers can begin filing their tax returns as early as mid-January. In its Fiscal Year 2015 Revenue Proposal, the IRS once again included a request for a legislative proposal to accelerate the deadline for filing third-party income and withholding information returns and eliminate the extended due date for electronically filed information returns.

In continuing our assessment of the IRS's identification of fraudulent tax returns involving identity theft, we initiated a review in August 2015 to follow-up on the IRS's identity theft detection and prevention efforts, including assessing the IRS's efforts to quantify undetected identity theft through its Taxonomy project.[6] The Taxonomy project aggregates the impact and loss of identity theft protection efforts across several IRS organizations and its goal is to achieve the level of precision and completeness required to provide critical strategic insights on identity theft affecting tax administration. We plan to issue our report by December 2016.

Question. Mr. George, in your testimony you note that there are 44 recommendations by TIGTA to the IRS in the area of information security that the IRS has yet to implement. Do you believe that these are recommendations the IRS can implement within its current budget? Has the IRS made a commitment to TIGTA to implement these recommendations?

Answer. We cannot definitively answer whether the IRS can implement our recommendations as it is up to the IRS to prioritize its planned corrective actions.

As of June 15, 2015, the IRS reported that it had recently closed eight of the 44 recommendations cited in our testimony. Of the 36 remaining recommendations, the IRS indicated in its response to our report that the completion of corrective actions in response to two of these recommendations may be contingent on available funding: (1) identifying funding needed to support implementation of a Homeland Security Directive to require Personal Identity Verification card access to the IRS network and information systems;[7] and (2) fully implementing software that will enable

---

[5] The calendar year in which the tax return or document is processed by the IRS.

[6] TIGTA, Audit No. 201540001, *Detection and Prevention of Identity Theft on Individual Tax Accounts—Follow-Up,* report planned for Dec. 2016.

[7] TIGTA, Ref. No. 2014–20–069, *Progress Has Been Made; However, Significant Work Remains to Achieve Full Implementation of Homeland Security Presidential Directive* (Sept. 2014).

the IRS to identify where its most sensitive data are stored, who has access to the data, and where and by whom the data are sent to outside the IRS network.[8]

As part of our audit process, the IRS can either agree or disagree with our audit recommendations. When it agrees, the IRS commits that they will correct the deficiency that we identified. In a prior audit, we assessed whether closed corrective actions to security weaknesses and findings reported by TIGTA had been fully implemented, validated, and documented as implemented.[9] During our audit, we determined that eight (42 percent) of 19 corrective actions that were approved and closed as fully implemented to address reported security weaknesses from prior TIGTA audits were only partially implemented. These corrective actions involved systems with taxpayer data.

On occasion, the IRS will disagree with our audit recommendations. In fact, during the last three fiscal years (Fiscal Years 2012 to 2014), the IRS disagreed with 10 of our 109 recommendations relating to information security in the following reports.

- *Using SmartID Cards to Access Computer Systems Is Taking Longer Than Expected* (Ref # 2012–20–115, dated September 28, 2012). The IRS disagreed with two of nine recommendations.
- *Improvements Are Needed to Ensure the Effectiveness of the Privacy Impact Assessment Process* (Ref # 2013–20–023, dated February 27, 2013). The IRS disagreed with two of 11 recommendations.
- *Better Cost-Benefit Analysis and Security Considerations Are Needed for the Bring Your Own Device Pilot Project* (Ref # 2013–20–108, dated September 24, 2013). The IRS disagreed with one of five recommendations.
- *While Efforts Are Ongoing to Deploy A Secure Mechanism to Verify Taxpayer Identifies, the Public Still Cannot Access Their Tax Account Information Via the Internet* (Ref # 2013–20–127, dated September 25, 2013). The IRS disagreed with one of four recommendations.
- *Improved Controls Are Needed to Ensure All Planned Corrective Actions for Security-Related Weaknesses Are Fully Implemented to Protect Taxpayer Data* (Ref # 2013–20–117, dated September 27, 2013). The IRS disagreed with one of six recommendations.
- *Planning is Underway for the Enterprise-Wide Transition to Internet Protocol Version 6 but Further Actions Are Needed* (Ref # 2014–20–016, dated February 27, 2014). The IRS disagreed with two of seven recommendations.
- *While the Data Loss Prevention Solution Is Being Developed, Stronger Oversight and Process Enhancements Are Needed for Timely Implementation Within Budget* (Ref # 2014–20–087, dated September 22, 2014). The IRS disagreed with one of 12 recommendations.

QUESTION SUBMITTED BY HON. THOMAS R. CARPER

Question. Please provide additional information on the cost of critical pay at the Internal Revenue Service (IRS).

Answer. TIGTA determined that the extra salary costs of the Streamlined Critical Pay program totaled approximately $1.7 million over the period reviewed (Calendar Years 2010 through 2013). The average pay of the highest graded Senior Executive Service Positions (ES–6) was approximately $179,000 a year while the average pay for the Streamlined Critical Pay positions was $ 198,000.

PREPARED STATEMENT OF HON. ORRIN G. HATCH, A U.S. SENATOR FROM UTAH

WASHINGTON—Senate Finance Committee Chairman Orrin Hatch (R–Utah) today delivered the following opening statement at a committee hearing regarding the data theft at the Internal Revenue Service (IRS) which compromised the private information of over 100,000 taxpayers:

---

[8] TIGTA, Ref. No. 2014–20–087, *While the Data Loss Prevention Solution Is Being Developed, Stronger Oversight and Process Enhancements Are Needed for Timely Implementation Within Budget* (Sept. 2014).

[9] TIGTA, Ref. No. 2013–20–117, *Improved Controls Are Needed to Ensure That All Planned Corrective Actions for Security Weaknesses Are Fully Implemented to Protect Taxpayer Data* (Sept. 2013).

Our hearing today concerns recent revelations that the Internal Revenue Service was the target of an organized service breach aimed at roughly 200,000 taxpayer accounts. We understand that over 100,000 of these breaches were successful, with cyber-criminals obtaining confidential taxpayer information from the agency's Get Transcript application.

In dealing with this breach here in the Senate, this Committee stands alone, having legislative jurisdiction over the Internal Revenue Code, oversight jurisdiction over the IRS, and wide-ranging abilities to conduct investigations dealing with individual taxpayer information.

While I have raised questions in the past about the way the IRS prioritizes its spending, today's hearing is about finding out how criminals stole vast amounts of taxpayer information. Any questions regarding funding levels for the agency should wait until we have a complete understanding about what occurred.

Before we turn to the technological issues, let's focus for a moment on the victims. Because of this breach, criminals were able to get personal information about roughly 104,000 taxpayers, potentially including Social Security Numbers, bank account numbers, and other sensitive information. These taxpayers, and their families, must now begin the long and difficult process of repairing their reputations. And they must do so with the knowledge that the thieves who stole their data will likely try to use it to perpetrate further fraud against them.

Commissioner Koskinen, put simply, your agency has failed these taxpayers.

This hearing is of utmost importance as we work to find out what individuals and organizations were behind this breach; discover how this breach occurred, and what steps the IRS might have taken to prevent it; find out what taxpayer information was compromised, and how this may affect both taxpayers and tax administration going forward; and determine what tools and resources are necessary to better protect taxpayers, catch cyber-criminals, and prevent this type of breach from being successful in the future.

Most of all, we must pledge to work together to make sure that this type of breach does not happen again.

The secure movement of information is the lifeblood of international commerce and a necessary predicate for efficient government administration. Unfortunately, this information is also highly valuable to criminals.

We see it in the headlines nearly every week—a major insurance company, bank, or retailer, has its information security compromised and personal information or corporate data is stolen. Federal departments—especially defense related agencies—come under attack each and every day.

The IRS is not, and will never be, exempted from this constant threat.

In fact, there is reason to believe the IRS will be more frequently targeted in the future. After all, the IRS stores highly sensitive information on each and every American taxpayer, from individual taxpayers to large organizations and from mom and pop businesses to multinational corporations. The challenge of data security matters a great deal to every single taxpayer and will continue to be a central challenge to tax administration in the coming years.

Of course, data security and the protection of taxpayer information are of the highest importance in the prevention of stolen identity refund fraud. Identity theft, and the resulting tax fraud, costs taxpayers billions of dollars every year, and, once it occurs, it can take months or years for a taxpayer to mitigate the damage.

It was out of concern over stolen identity refund fraud that Ranking Member Wyden and I quietly launched an investigation earlier this year, requesting information and documents from the country's largest tax return preparers and debit card companies.

We look forward to working with the IRS as we move forward with this investigation and consider policy changes. We also look forward to hearing the report from your preparer working groups, and the committee looks forward to weighing in on those matters in the near future.

So I welcome our witnesses today, IRS Commissioner Koskinen and Inspector General George. Commissioner Koskinen, earlier this year, when I first welcomed you before the Committee as Chairman, I noted that I hoped it would be the beginning of a new chapter in the long, historic relationship between the Internal Revenue Service and the Senate Finance Committee. I said that because the issues be-

fore us are too great for that relationship to be anything but open, honest, and productive.

Today's topic is a great example of why that relationship is so important. Cyberthreats will only continue to grow, and those types of threats go to the core of our voluntary tax system. We must work together to figure out what happened, what went wrong in allowing the breach to occur, and how we can prevent another successful attack from taking place in the future.

Finally, I would like to acknowledge that today's hearing occurs during somewhat unusual circumstances.

The issue before us is the subject of several recently opened investigations, including a criminal investigation conducted by TIGTA. I caution members of the committee to be sensitive to these investigations when asking questions of the witnesses, and be aware that they may not be able to provide full answers to every question in this public forum. In spite of these limitations, it is important to discuss this matter today as fully and candidly as possible.

PREPARED STATEMENT OF HON. JOHN A. KOSKINEN, COMMISSIONER, INTERNAL REVENUE SERVICE

Chairman Hatch, Ranking Member Wyden, and members of the committee, thank you for the opportunity to appear before you today to provide information on the recent unauthorized attempts to obtain taxpayer data through the IRS's Get Transcript online application.

While we are continuing our in-depth analysis of what happened, the analysis thus far has found that the unauthorized attempts to request information from the Get Transcript application were complex and sophisticated in nature. These attempts were made using taxpayers' personal information already obtained from sources outside the IRS—meaning the parties making the attempts had enough information to clear the Get Transcript application's multi-step authentication process.

For now, our biggest concern is for the affected taxpayers, to make sure they are protected against fraud in the future. We recognize the severity of the situation for these taxpayers, and we are doing everything we can to help them.

Securing our systems and protecting taxpayers' information is a top priority for the IRS. Even with our constrained resources as a result of cuts to our budget totaling $1.2 billion since 2010, we continue to devote significant time and attention to this challenge. At the same time, it is clear that criminals have been able to gather increasing amounts of personal data as the result of data breaches at sources outside the IRS, which makes protecting taxpayers increasingly challenging and difficult.

The problem of personal data being stolen from sources outside the IRS to perpetrate tax refund fraud exploded from 2010 to 2012, and for a time overwhelmed law enforcement and the IRS. Since then, we have been making steady progress, both in terms of protecting against fraudulent refund claims and prosecuting those who engage in this crime. Over the past few years, almost 2,000 individuals were convicted in connection with refund fraud related to identity theft. The average prison sentence for identity theft-related tax refund fraud grew to 43 months in Fiscal Year (FY) 2014 from 38 months in FY 2013, with the longest sentence being 27 years.

Additionally, as our processing filters have improved, we have also been able to stop more suspicious returns at the door, rather than accepting them for processing. This past filing season, our fraud filters stopped almost 3 million fraudulent returns before processing them, an increase of over 700,000 from the year before. But, even though we have been effective at stopping individuals perpetrating these crimes, we find that we are dealing more and more with organized crime syndicates here and around the world.

At the same time, over the last several years, the IRS has been working to meet taxpayers' increasing demand for self-service and electronic service options by providing them with more web-based tools, to make their interactions with us simpler and easier. As part of that effort, we launched the Get Transcript online application in January 2014. Get Transcript allows taxpayers to view and print a copy of their prior-year tax information, also known as a transcript, in a matter of minutes. Prior

to the introduction of this online tool, taxpayers had to wait 5 to 7 days after placing an order by phone or by mail to receive a paper transcript by mail. Taxpayers use tax transcript information for a variety of financial activities, such as verifying income when applying for a mortgage or student loan.

To access Get Transcript, taxpayers must go through a multi-step authentication process to prove their identity, consistent with many organizations in the financial services industry. They must first submit personal information such as their Social Security Number (SSN), date of birth, tax filing status, and home address, as well as an e-mail address. The taxpayer then receives an e-mail from the Get Transcript system containing a confirmation code that they enter to access the application and request a transcript. Before the request is processed, the taxpayer must respond to several "out-of-wallet" questions—a customer authentication method that is standard within the financial services industry. The questions are designed to elicit information that only the taxpayer would normally know, such as the amount of their monthly mortgage or car payment.

During the 2015 filing season, taxpayers used the Get Transcript application to successfully obtain approximately 23 million copies of their recently filed tax information. If this application had not existed and these taxpayers had to call or write us to order a transcript, it would have stretched our limited resources even further. That is important to note, given our limitations during the past filing season. We would have been much less efficient in providing taxpayer service, not to mention the additional burden placed on taxpayers.

During the middle of May, our cyber-security team noticed unusual activity on the Get Transcript application. At the time, our team thought this might be a "denial of service" attack, where hackers try to disrupt a website's normal functioning. Our teams worked aggressively to look deeper into the situation during the following days, and ultimately uncovered questionable attempts to access the Get Transcript application.

As a result, the IRS shut down the Get Transcript application on May 21st. The application will remain disabled until the IRS makes modifications and further strengthens security for the application. It should be noted that the third parties who made these unauthorized attempts to obtain tax account information did not attempt to gain access to the main IRS computer system that handles tax filing submissions. The main IRS computer system remains secure, as do other online IRS applications such as "Where's My Refund?" Unlike Get Transcript, the other online applications do not allow taxpayers to access their personal tax data.

As they continued to investigate, our team determined that a total of approximately 200,000 suspicious attempts to gain access to taxpayer information on the Get Transcript application had been made between mid-February and mid-May. About 100,000 of the attempts were unsuccessful, with the parties making these attempts unable to work their way through the protections in place.

But we know that the other 100,000 or so attempts to request information from the Get Transcript application between mid-February and mid-May were successful. We are analyzing what, if anything, was done with the personal information of these taxpayers obtained using the Get Transcript application, and have discovered the following:

- About 35,000 taxpayers had already filed their 2014 income tax returns before the unauthorized attempts at access. This means that these taxpayers' 2014 returns and refund claims were not affected by this fraudulent activity, because any fraudulent return subsequently filed in their names would be automatically rejected by our systems;
- For another 33,000, there is no record of any return having been filed in 2015. This could be the case for a number of reasons. For example, the SSNs associated with these individuals may belong to those who have no obligation to file, such as children, or anyone below the tax filing threshold;
- Unsuccessful attempts were made to file approximately 23,500 returns. These 23,500 returns were flagged by our fraud filters and stopped by our processing systems before refunds were issued; and
- Since this activity occurred, about 13,000 suspect returns were filed for tax year 2014 for which the IRS issued refunds. Refunds issued for these 13,000 suspect returns totaled about $39 million, and the average refund was approximately $3,000 per return. We are still determining how many of these returns were filed by the actual taxpayers and which were filed using stolen identities. We

will work with any of these affected taxpayers who had fraudulent returns filed in their name.

As I mentioned at the outset, our analysis thus far has found that the unauthorized attempts to access information using the Get Transcript application were complex and sophisticated in nature. These attempts were made using personal information already obtained from sources outside the IRS—meaning the parties making the attempts had enough information to clear the Get Transcript application's multi-step authentication process, including answers to the out-of-wallet questions.

We believe it is possible that some of the attempts to access tax transcripts were made with an eye toward using the information to file fraudulent tax returns next year. For example, any prior-year return information criminals obtain would help them more easily craft seemingly authentic returns, making it more difficult for our filters to detect the fraudulent nature of the returns.

As noted above, since we have already disabled Get Transcript, our biggest concern right now is for the affected taxpayers, to make sure they are protected against fraud in the future. We recognize the severity of the situation for these taxpayers, and have taken a number of immediate steps to assist the affected taxpayers in protecting their data against fraud that might be perpetrated against them. First, we have placed an identifier on the accounts of the roughly 200,000 affected taxpayers on our core tax account system to prevent someone else from filing a tax return in their name—both now and in future years.

Second, we are in the process of writing to all 200,000 taxpayers to let them know that third parties appear to have gained access from outside the IRS to personal information such as their SSNs, in an attempt to obtain their tax information from the IRS. Although half of this group did not actually have their transcript accessed because those who were trying to gain this information failed the authentication tests, the IRS believes it is important to make these taxpayers aware that someone else has their personal data. We want them to be able to take steps to safeguard their data.

Letters have already been sent to all of the approximately 100,000 taxpayers whose tax information was successfully obtained by unauthorized third parties. We are offering credit monitoring, at our expense, to this group of taxpayers. We strongly encourage people who receive this letter to take advantage of this offer. We are also giving them the opportunity to provide us with the authentication documentation necessary to obtain an Identity Protection Personal Identification Number (IP PIN). This will further safeguard their IRS accounts and help them avoid any problems filing returns in future years.

As further analysis is done, we may uncover evidence that personal information of others, such as spouses and dependents of the taxpayers already identified, was also compromised, and we will take similar steps to protect those individuals.

More broadly, the IRS continues to work to help taxpayers who have been victims of identity theft. For example, for the 2015 filing season, the IRS has issued IP PINs to 1.5 million taxpayers previously identified by the IRS as victims of identity theft. Also during this period, the IRS notified another 1.7 million taxpayers that they were eligible to visit IRS.gov and opt in to the IP PIN program. Meanwhile, taxpayers living in Florida, Georgia, and Washington, DC—three areas where there have been particularly high concentrations of identity-theft related refund fraud—are eligible to participate in a pilot where they can receive an IP PIN upon request, regardless of whether the IRS has identified them as a victim of identity theft.

In terms of our investigative work on identity theft, it is important to note that our Criminal Investigation (CI) division has seen an increase in identity theft crime being perpetrated by organized crime syndicates. The IRS is working closely with law enforcement agencies in the U.S. and around the world to prosecute these criminals and protect taxpayers. But the fact remains that these cyber-criminals are increasingly sophisticated enemies, with access to substantial volumes of data on millions of people.

For that reason, we recently held a sit-down meeting with the leaders of the tax software and payroll industries and state tax administrators, and agreed to build on our cooperative efforts of the past and find new ways to leverage this public-private partnership to help battle identity theft. The working groups that were formed out of this meeting have continued to meet, and later this month we expect to announce an agreement on short-term solutions to help better protect personal

information in the upcoming tax filing season, and to continue to work on longer-term efforts to protect the integrity of the nation's tax system.

One of the three working groups formed out of this meeting focuses on authentication. As criminals obtain more personal information, authentication protocols need to become more sophisticated, moving beyond information that used to be known only to individuals but now, in many cases, is readily available to criminal organizations from various sources. We must balance the strongest possible authentication processes with the ability of taxpayers to legitimately access their data and use IRS services online. The challenge will always be to keep up with, if not get ahead of, our enemies in this area.

Congress has an important role to play here. Congress can help by approving the President's FY 2016 Budget request, which includes $101 million specifically devoted to identity theft and refund fraud, plus $188 million for critical information technology infrastructure. Along with providing adequate funding, lawmakers can help the IRS in the fight against refund fraud and identity theft by passing several important legislative proposals in the President's FY 2016 Budget proposal. A key item on this list is a proposal to accelerate information return filing dates.

Under current law, most information returns, including Forms 1099 and 1098, must be filed with the IRS by February 28 of the year following the year for which the information is being reported, while Form W–2 must be filed with the Social Security Administration (SSA) by the last day of February. The due date for filing information returns with the IRS or SSA is generally extended until March 31st if the returns are filed electronically. The Budget proposal would require these information returns to be filed when copies of this information are provided to the taxpayers, generally by January 31st of the year following the year for which the information is being reported, which would assist the IRS in identifying fraudulent returns and reduce refund fraud related to identity theft.

There are a number of other legislative proposals in the Administration's FY 2016 Budget that would also assist the IRS in its efforts to combat identity theft, including: giving Treasury and the IRS authority to require or permit employers to mask a portion of an employee's SSN on W–2s, which would make it more difficult for identity thieves to steal SSNs; adding tax-related offenses to the list of crimes in the Aggravated Identity Theft Statute, which would subject criminals convicted of tax-related identity theft crimes to longer sentences than those that apply under current law; and adding a $5,000 civil penalty to the Internal Revenue Code for tax-related identity theft cases, to provide an additional enforcement tool that could be used in conjunction with criminal prosecutions.

Chairman Hatch, Ranking Member Wyden, and members of the committee, thank you again for the opportunity to provide information on the recent unauthorized attempts to obtain taxpayer data through the IRS's Get Transcript online application. This concludes my statement, and I would be happy to take your questions.

QUESTIONS SUBMITTED FOR THE RECORD TO HON. JOHN A. KOSKINEN

QUESTIONS SUBMITTED BY HON. DEAN HELLER

Question. The recent IRS data breach of 104,000 victims only emphasizes how tax schemes, such as identity theft and return preparer fraud, are on the rise. For the 2014 tax year, it is estimated there have been close to 2 million in confirmed tax related identity thefts. In my home state alone, there have been over 14,000 victims. These numbers are disturbing, but what is more upsetting is the complex and frustrating process that these innocent victims are put through. It is my understanding refunds can take almost a year to get back to the true taxpayer. For this recent data breach, how is the IRS addressing the affected taxpayers, especially the ones where a return had been illegally filed and a refund issued?

Answer. We realize the importance of resolving cases involving identity theft quickly and efficiently, thus allowing taxpayers victimized by identity theft to receive their refunds as soon as possible and helping to reduce the risk that adverse enforcement actions will be taken against them. To that end, we continue to develop and implement new procedures to improve the service provided to identity theft victims.

Due to the complexity of these situations, identity theft victim case resolution can be a time-consuming process. However, the IRS has successfully reduced the case-

processing and resolution time for identity-theft cases to improve service to the taxpayer. During the past fiscal year, taxpayers who became identity theft victims had their situations resolved in roughly 120 days, far more quickly than in previous years, when cases could take over 300 days to resolve. The IRS continues to evaluate systems and processes to improve the taxpayer experience.

The IRS continues to expand its outreach initiatives to provide taxpayers, return preparers, state tax agencies, and other stakeholders with the information they need to prevent tax-related identity theft and, when identity theft does occur, to resolve issues as quickly and efficiently as possible. We also partner with other federal agencies to further these outreach efforts.

Ensuring the security of our systems and the protection of taxpayers and their information are top priorities. Even with our constrained resources over the past few years, we continue to devote significant time and attention to these challenges. Ongoing data breaches involving other companies and organizations, through which criminals have been able to gather increasing amounts of personal data, make it even more challenging and difficult to protect taxpayers.

You asked how the IRS is addressing the taxpayers affected by the recent unauthorized-access incident involving the Get Transcript application. In May, the IRS determined unauthorized third parties already had sufficient information from a source outside the tax agency before accessing the Get Transcript application. This allowed them to clear a multi-step authentication process, including several personal verification questions that typically are only known by the taxpayer.

When the IRS first identified the problem in May, we determined that these third parties with taxpayer-specific sensitive data from non-IRS sources had cleared the Get Transcript verification process on about 114,000 total attempts. In addition, it appeared at that time that third parties had made attempts that failed to pass the final verification step, meaning they were unable to access account information through the Get Transcript service.

Since then, as part of the IRS's continued efforts to protect taxpayer data, the IRS conducted a deeper analysis over a wider time period covering the 2015 filing season, analyzing more than 23 million uses of the Get Transcript system. The new review identified an estimated additional 220,000 attempts where individuals with taxpayer-specific sensitive data cleared the Get Transcript verification process. The review also identified an additional 170,000 suspected attempts that failed to clear the authentication processes.

The IRS mailed letters to all taxpayers identified in May and, later, we also mailed letters to the population identified in August as part of our continued analysis. To the taxpayers whose tax information was successfully obtained by unauthorized third parties, we are offering credit monitoring, at our expense. We strongly encourage the recipients of these letters to take advantage of the credit monitoring. We are also giving them the opportunity to provide us with the authentication documentation necessary to get an Identity Protection Personal Identification Number (IP PIN). This will further safeguard their IRS accounts and help them avoid any problems filing returns in future years. The IRS is marking all of the affected accounts with indicators that will help identify and prevent any fraudulent returns from being filed under those Social Security Numbers (SSN).

The Get Transcript application was shut down in May, and the IRS continues to work on strengthening the system. In the meantime, taxpayers have several other options to obtain transcripts.

The IRS takes the security of taxpayer data extremely seriously, and we are working aggressively to protect affected taxpayers and continue to strengthen our systems.

The matter remains under review by the Treasury Inspector General for Tax Administration as well as IRS Criminal Investigation.

Question. I understand that the IRS is considering allowing these individuals to receive a secure PIN, also known as the IP PIN, as part of an IRS pilot program. Could a secure PIN be provided to all taxpayers? If not, why not?

Answer. The Identity Protection Personal Identification Number (IP PIN) is one component of the IRS arsenal to combat identity theft and fraud. We have many other tools and solutions in use and under development to increase security of taxpayer data.

We are conducting research and analysis to determine the feasibility of expanding the IP PIN program. Although additional expansion of the IP PIN program may help safeguard more taxpayers from tax-related identity theft and refund fraud, it would require a substantial investment of financial resources which are not available at this time.

Question. Public trust is crucial to the IRS's success. I was disturbed to understand that a recent GAO report found that a number of weaknesses, to effectively protect taxpayers' confidentiality, integrity and availability of sensitive taxpayer data, had not been implemented. My understanding is that less than a third of changes were implemented remain open between the last GAO audit and this year. How can the committee or taxpayers have faith in the IRS, if significant deficiencies in internal controls are not being addressed? Follow-up when do you expect to have these weaknesses addressed?

Answer. The security and privacy of taxpayer information and the integrity of our computer systems continue to be sound. Our Cyber-security program provides proactive defenses by implementing world-class security practices in planning, implementation, management, and operations involving people, process, and technologies. We continually monitor the security controls in our information systems and the environments in which those systems operate. We also maintain awareness of information security, vulnerabilities, and threats to support organizational risk management decisions. We remain committed to our ongoing programs to manage the security risks in our IT infrastructure in accordance with industry standards and as required by the Federal Information Security Management Act (FISMA) and the National Institute of Standards and Technology guidance, and we continue to decrease the number of our unresolved weaknesses.

We are working diligently to address all of the findings identified by GAO. The IRS has submitted 31 of the 79 open findings to GAO for closure during the FY 2015 audit. Currently, up to 30 of the remaining open items are in progress and scheduled to be submitted to GAO for closure in FY 2016. The balance of the open findings are scheduled for closure by FY 2019. It should be noted that GAO's recommendations do not concern fundamental weaknesses in taxpayer-facing systems. Rather, they concern weaknesses in our controls for internal systems—that is, systems and data that are behind our portal and firewalls. These systems have less risk of experiencing security issues because they are not connected directly to the external internet. In addition, factors such as budget uncertainties, hiring freezes, skillset deficits, and complexities associated with our antiquated legacy environment, as well as cutbacks affecting our ability to update our infrastructure, must also be considered. Nonetheless, we continue to review and evaluate all of GAO's recommendations along with other outstanding recommendations in light of risk and security controls and processes currently in place. We are building corrective action plans where appropriate to address the recommendations, and we are prioritizing and addressing them as resources permit. Significant progress has been made in addressing these recommendations in areas where we are most vulnerable.

Our efforts to install software patches for security vulnerabilities continue to improve with the implementation of newer releases of more efficient and effective patching tools. We are developing our enterprise-wide processes to deliver software patches across all of our environments. This extensive effort continues to improve our vulnerable systems and the timeliness of patching provided by our patching teams. These improvements have been realized in spite of increasing challenges such as more sophisticated attackers, increased system complexity in our environments, and loss of some of our most experienced staff. While some patch management activities may take longer than we would like due to funding reductions, resource constraints, and the complexity of our environments, we expect to address the GAO findings related to patch management in FY 2016 as we continue to improve the program.

We are making steady progress in closing vulnerabilities and addressing GAO findings associated with passwords. We have implemented standards that create systemic fixes for common issues in creating employee and administrator passwords. We also conduct monthly vulnerability scanning to ensure systems compliance with the password policy. Although we have not had sufficient funding and capacity to implement the Homeland Security Presidential Directive (HSPD)–12 initiative as quickly as we would like, we are continuing to transition from using passwords to using the Personal Identity Verification (PIV) card for system sign-on for all users. This required substantial effort due to the number of systems that need updating, the advanced age of some of these systems, the complexity of system interactions,

and the high cost to update them. We expect 100% of users with regular access privileges to be HSPD–12 ready by the end of FY 2016.

We are enhancing our auditing and monitoring capabilities by dedicating our limited resources in this area to our highest risk systems. This will help us track security violations and confirm individual accountability. In FY 2014, we developed a risk-based prioritization strategy to align the schedules of systems needing audit trails. Since FY 2014, we have been dedicating significant financial resources to ensure all new systems are implemented with audit trails, and to expand the audit trails infrastructure capacity to support the new data collection. We have prioritized the audit trails findings in the GAO report and we expect that the systems documented in the report will be completed in FY 2016 and FY 2017.

Question. The Committee held a hearing, earlier this year, on tax scams including identity theft, "Protecting Taxpayers from Schemes and Scams during the 2015 Filing Season." Mr. Alley, the Commissioner of the Indiana Department of Revenue, stressed that the identity confirmation quiz was a significant and powerful tool to combat ID fraud. Has the IRS considered implementing a similar procedure such as this to reduce tax scams?

Answer. The IRS currently uses an identity-confirmation quiz, called out-of-wallet questions, to authenticate taxpayers. The name refers to questions that would not be easily answerable with the information in a person's wallet if it were stolen.

The IRS is reviewing multiple-authentication policy and capabilities in response to the unauthorized disclosures associated with the Get Transcript application. We are researching internal capabilities as well as those available from third parties through existing and planned contracts. These options include, but are not limited to:

- Third-party configuration changes to strengthen out-of-wallet questions;
- Internal IRS configuration updates to limit fraud and vulnerabilities to scripting attacks;
- Additional levels of assurance and authentication points; and
- Additional risk-based authentication capabilities.

We must balance the strongest possible authentication processes with the ability of taxpayers to legitimately access their data and use IRS services online. The challenge will always be to keep up with, if not get ahead of, fraudsters in this area.

Question. In Mr. Alley's testimony, he also focused on how the identity confirmation quiz is only part of a larger process to strategically focus on identity theft and refund fraud. This encompassed hiring additional talent, implementing new procedures and new IT systems and conducting a public relations campaign. What steps are the IRS taking to address identity theft?

Answer. The IRS has a comprehensive and aggressive identity-theft strategy focused on preventing refund fraud, investigating these crimes, and assisting taxpayers victimized by identity thieves. We are also continuously conducting analysis and looking for ways to improve identity-theft detection. Because identity-theft criminals have significant resources to devote to these schemes, their methods are constantly evolving, forcing us to continually adjust our filters and processes accordingly.

Realizing that we are only one stakeholder in the battle against identity theft, in March we organized a Security Summit that included representatives from the IRS, state tax agencies and private industry, such as software vendors, to work on collaborative solutions to combat fraud schemes. The Summit established a new public/private partnership effort to combat identify theft, refund fraud and protect the nation's taxpayers. In addition, participants reached agreement on several initiatives to address identity theft. These initiatives were announced on June 11, 2015. The agreement includes identifying new steps to validate taxpayer and tax return data at the time of filing. The effort will increase information sharing between industry and government. This public/private partnership is continuing to work on initiatives to be implemented in 2017 and beyond.

In addition to victim assistance and outreach, the IRS's identity theft strategy also focuses on preventing refund fraud and investigating these crimes. Additional initiatives include these FY 2015 items:

- We now limit the number of tax refund deposits to a single account to three (3). Additional refunds to the same account are converted to paper checks. We

believe this initiative has had a positive impact on our efforts to deter fraud and identity theft.

- We began receiving device ID information to identify potential identity theft or fraud. The device ID is the serial number (or fingerprint) of the device (for example, computer, smart phone, or tablet). The unique ID is transmitted as part of the electronically filed return via our existing transmission process and enables the IRS to associate fraudulent returns that are filed from the same device.
- In addition to the nearly 1.5 million taxpayers that are given an Identity Protection Personal Identification Number (IP PIN), we expanded the population eligible for IP PINs to taxpayers previously identified by the IRS as victims of identity theft. This allowed approximately 1.7 million more taxpayers to opt in to the IP PIN program.
- We continue to accelerate the use of more types of information returns to identify mismatches earlier.
- We provide phone, online and in person channels to enable taxpayers inadvertently caught up in our protective filters to validate their identity and have their return processed. We continue to implement new identity theft screening filters to improve our ability to spot false returns before we process them and issue refunds.

The IRS also continues to collaborate with software companies and financial institutions to identify patterns, trends and schemes that affect refund returns.

The IRS also has initiated additional collaboration with the Bureau of Fiscal Service (BFS) on multiple direct deposits and payments shared between government agencies in the development of the new Payment Processing System. This collaboration provides an opportunity for IRS and other government agencies to work through BFS to identify fraudulent payments, increase recovery opportunities, improve data access, and reduce time in extracting or analyzing information from multiple data sources. This will also afford the opportunity for IRS and BFS to collaborate on refunds that have made it through IRS systems but appear suspicious based upon additional information and data external to IRS. The BFS system is expected to be online in September 2016.

In addition, Congress can help us in the fight against refund fraud and identity theft, by enacting several important legislative proposals in the President's FY 2016 Budget proposal, including the following:

- **Acceleration of information return filing due dates.** Under current law, most information returns, including Forms 1099 and 1098, must be filed with the IRS by February 28th of the year following the year for which the information is being reported, while Form W–2 must be filed with the Social Security Administration (SSA) by the last day of February. The due date for filing information returns with the IRS or SSA is generally extended until March 31st if the returns are filed electronically. The Budget proposal would require these information returns to be filed earlier, which would assist the IRS in identifying fraudulent returns and reduce refund fraud, including refund fraud related to identity theft.
- **Correctible error authority.** The IRS has authority in limited circumstances to identify certain computation or other irregularities on returns and automatically adjust the return for a taxpayer, colloquially known as "math error authority." At various times, Congress has expanded this limited authority on a case-by-case basis to cover specific, newly enacted tax code amendments. The IRS would be able to significantly improve tax administration—including reducing improper payments and refund fraud as well as cutting down on the need for costly audits—if Congress were to enact the Budget proposal to replace the existing specific grants of this authority with more general authority covering computation errors and incorrect use of IRS tables. Congress could also help in this regard by creating a new category of "correctable errors," allowing the IRS to fix errors in several specific situations, such as when a taxpayer's information does not match the data in certain government databases. To correct these errors today, IRS must open an audit, and we are limited in the number of audits we conduct by the resources available to engage with the taxpayer in the full audit process. Being able to correct certain mismatch errors would help with reducing some types of refund fraud.

- **Authority to ensure minimum qualifications for return preparers.** In the wake of court decisions striking down the IRS's authority to regulate unenrolled and unlicensed paid tax return preparers, Congress should enact the Budget proposal to provide the agency with explicit authority to ensure paid preparers maintain minimum qualifications. This authority would help promote high quality services from tax return preparers, reduce refund fraud, improve voluntary compliance, foster taxpayer confidence in the fairness of the tax system, and protect taxpayers from preparer errors.
- **Expanded access to Directory of New Hires.** Under current law, the IRS is permitted to access the Department of Health and Human Services' National Directory of New Hires only for purposes of enforcing the Earned Income Tax Credit and verifying employment reported on a tax return. The proposal would allow IRS access to the directory for tax administration purposes that include data matching, verification of taxpayer claims during return processing, preparation of substitute returns for non-compliant taxpayers, and identification of levy sources.

There are a number of other legislative proposals in the Administration's FY 2016 Budget request that would also assist the IRS in its efforts to combat identity theft, including: giving Treasury and the IRS authority to require or permit employers to mask a portion of an employee's SSN on W–2s, which would make it more difficult for identity thieves to steal SSNs; adding tax-related offenses to the list of crimes in the Aggravated Identity Theft Statute, which would subject criminals convicted of tax-related identity theft crimes to longer sentences than those that apply under current law; and adding a $5,000 civil penalty to the Internal Revenue Code for tax-related identity theft cases, to provide an additional enforcement tool that could be used in conjunction with criminal prosecutions.

It is important to note that these legislative proposals, while they would be very helpful, only would be partially effective in achieving their intended goals without adequate resources for the agency.

With limited resources and information, the IRS currently is only able to review fewer than 5% of the 100 million returns that request a refund. If, prior to issuing refunds, the IRS had access to third-party documents for matching earlier in the filing season (*e.g.,* W–2), we would be able to stop more refund fraud.

With additional resources, the IRS could implement the following improvements to protect revenue and taxpayers:

- Expand the pre-refund filters and improve systemic coverage of potential ID Theft returns;
- Increase the number of analysts manually reviewing filing patterns to identify new suspicious patterns and react to newly submitted leads; and
- Improve service to victims of identity theft by increasing the number of IRS employees who manually review returns, contact taxpayers when needed, and make account adjustments for taxpayers affected by ID Theft.

Question. During the summer of 2012, the IRS worked with an incumbent consulting firm to conduct tests of third-party, commercially available analytics to determine how well those solutions could detect and prevent fraudulent tax returns. What were the results of those tests and if they were successful, why have none of those solutions been implemented?

Answer. In 2012, the IRS conducted a study to determine if third-party, commercially available analytics might improve identity theft protection beyond existing IRS Identity Theft (IDT) capabilities. Today, the IRS uses third-party data to facilitate validating identities and deterring ID theft fraud. For example, the Taxpayer Protection Program currently uses a third-party vendor's data to support ID Verify challenge questions used to authenticate taxpayers whose returns appear to be compromised by identity theft. In addition, the IRS is further partnering with industry to determine if new data sources and data elements can help IRS increase identity theft detection capabilities.

Question. Does IRC 7216 need to be permanently amended to allow for the disclosure of limited filer information for the purposes of preventing fraudulent returns?

Answer. Section 7216 does not require amendment to allow for the disclosure of limited filer information for purposes of preventing fraudulent returns. Regulations under section 7216 currently allow any disclosure of tax return information to an officer or employee of the IRS. Treas. Reg. § 301.7216–2(b). They also allow disclo-

sure of any tax return information to the proper Federal, State, or local officials to inform them of activities that may constitute a violation of any criminal law or to assist the investigation or prosecution of a violation of criminal law. Treas. Reg. § 301.7216–2(q).

Question. Has the IRS considered allowing consumers to opt into an alerting service that would notify them whenever a tax return has been filed using a consumer's personal information?

Answer. Given current funding limitations, the IRS does not plan to implement an opt-in plan to notify a taxpayer whenever a tax return has been filed using a taxpayer's SSN or Individual Taxpayer Identification Number (ITIN). Currently, taxpayers are contacted when an individual tax return passes through IRS filters and is flagged for potential identity theft.

QUESTIONS SUBMITTED BY HON. DEBBIE STABENOW

Question. Over the last couple of years, we have seen several large data breaches involving tens of millions of customers: Target—40 million people, JPMorgan—76 million people, Home Depot—56 million people, Anthem—80 million people.

The information stolen in the large data breaches is the kind of information that is then used to file false tax returns to obtain refunds, or, in this case, to access taxpayer information through the IRS. It emphasizes the need for greater security throughout the payment chain, before identity thieves get to the point of using stolen information to file false returns.

As Commissioner of the IRS, you are limited in your ability to combat certain kinds of identity theft because you don't have control over the payment chain—identity thieves are using information that they have already obtained to file fraudulent returns.

Can you tell us more about some of the steps that the IRS has been exploring to protect against fraudulent returns?

Answer. The IRS has a comprehensive and aggressive identity theft strategy focused on preventing refund fraud, investigating these crimes, and assisting taxpayers victimized by identity thieves. We are also continuously conducting analysis and looking for ways to improve identity theft detection. Because identity theft criminals have significant resources to devote to these schemes, their methods are constantly evolving, forcing us to continually adjust our filters and processes accordingly. Realizing that we are only one participant in the battle against identity theft, we recently organized a Security Summit and invited representatives from state tax agencies and private industry, such as software vendors, to work on collaborative solutions to combat fraud schemes.

In addition to victim assistance and outreach, the IRS's identity theft strategy also focuses on preventing refund fraud and investigating these crimes. Additional initiatives include these FY 2015 items:

- We now limit the number of tax refund deposits to a single account to three (3). Additional refunds to the same account are converted to paper checks. We believe this initiative has had a positive impact on our efforts to deter fraud and identity theft.
- We began receiving Device ID information to identify potential identity theft or fraud. The Device ID is the serial number (or fingerprint) of the device (for example, Computer, Smart Phone or Tablet). The unique ID is transmitted as part of the electronically filed return via our existing transmission process and enables the IRS to associate fraudulent returns that are filed from the same device.
- In addition to the nearly 1.5 million taxpayers that are given an Identity Protection Personal Identification Number (IP PIN), we expanded the population eligible to opt-in for IP PINs to taxpayers previously identified by the IRS as victims of identity theft. This allowed approximately 1.7 million more taxpayers to opt in to the IP PIN program.
- We continue to accelerate the use of more types of information returns to identify mismatches earlier.

- We provide phone, online and in person channels to enable those taxpayers, inadvertently caught up in our protective filters, to validate their identities and have their return processed.
- We continue to implement new identity theft screening filters to improve our ability to spot false returns before we process them and issue refunds.

The IRS also continues to collaborate with software companies and financial institutions to identify patterns, trends and schemes that impact refund returns. The IRS also has initiated additional collaboration with the Bureau of Fiscal Service (BFS) on multiple direct deposits and payments shared between government agencies in the development of the new Payment Processing System. This collaboration provides an opportunity for IRS and other government agencies to work through BFS to identify fraudulent payments, increase recovery opportunities, improve data access, and reduce time in extracting or analyzing information from multiple data sources. This will also afford the opportunity for IRS and BFS to collaborate on refunds that have made it through IRS systems but appear suspicious based upon additional information and data external to IRS. The BFS system is expected to be online in September 2016.

Question. Over the last few years, TIGTA and GAO have issued a number of reports on data security at the IRS, identifying a great many vulnerabilities and making recommendations for how those vulnerabilities might be addressed.

While the IRS has made several efforts to implement recommendations and secure vulnerable information, follow-up reports suggest that many recommendations, those with which IRS agreed, remain unimplemented and many vulnerabilities still exist.

Can you tell us more about the difficulties that the IRS has experienced in securing taxpayer data and protecting against fraud?

Have any factors limited your ability to implement some of the measures you might want to take?

Answer. The IRS is confident that its systems demonstrate high resistance to the normal daily cyber-attacks seen across government. However, there are no absolutes and, as with nearly all such current commercial cyber-defenses, it is very difficult to defend against sophisticated technologies. The IRS continues to devote scarce resources to cyber-security but after five years of cuts to our budget, it is currently much more challenging for the IRS to continuously stay ahead of evolving threats to its cyber-security.

The IRS has been storing taxpayer data in digital form since 1970 and has a strong culture of protecting this data. Currently, the IRS takes a very aggressive approach to protecting taxpayer data through: restrictions on internet access; encryption of taxpayer data for any transmission externally; content filtering and strict firewall policies; and network security monitoring. In fact, the IRS has developed a Cyber-security Strategy that is focused on managing information security risk on a continuous basis; monitoring the security controls in IRS information systems and the environments in which those systems operate on an ongoing basis; and maintaining ongoing awareness of information security, vulnerabilities and threats.

The critical risk to continuing to implement this strategy is not the sophistication or frequency of cyber-attacks, but instead is the IRS's current budget situation which has resulted in the reduction of Cyber-security staff and the inability to fill vacant positions. These skill sets and talents are under high demand across both the public and private sectors. The IRS's Cyber-security staff is currently 356 personnel, which is down from its high of 408 employees in FY 2012. The inability to hire and retain certified Cyber-security staff prevents the IRS from sustaining its vigilance against cyber-attack. This creates a capacity issue within cyber-security, where there are simply too many priorities and not enough time and resources to do all the work that needs to be done. In this situation, even high risk initiatives are put on hold, which is certainly not optimal with a mission as critical as the IRS.

The IRS's current budget situation is also hampering our ability to modernize our antiquated systems and keep current our IT infrastructure, which is thwarting progress in implementing security controls and protecting us against today's cyber-attacks. For example, the design and logic of many of our IT systems dates back to the 1960s, and those systems simply do not support protective measures recommended by GAO and others that are needed in today's technological environment. Similarly, many of our off-the-shelf applications are running on older, less secure versions, and some are even reaching end-of-life and are no longer supported by the

software companies, meaning they are no longer receiving security and other patches to ward off cyber-attacks and performance issues.

Funding has clearly limited IRS's ability to improve data security. As explained further in response to the next question, fully funding the IRS's information-security operations at the levels specified in the President's FY 2016 Budget request would allow for significant improvements in data security at the IRS.

Question. Year after year, Congress has cut the budget of the IRS while asking you to take on more responsibility. We've given you less money and fewer employees with which to protect the information of so many millions of taxpayers across the country.

Some of my colleagues are fond of the saying: when you tax something you get less of it. However, I would point out that when you pay for less of something, you get less of it. When you pay less for data security, you get less data security. It's a pretty straightforward concept, but unfortunately, here we are, after five years of cutting the IRS budget, being concerned about why more resources weren't put into data security.

Commissioner Koskinen, if this Committee and this Congress would give you more tools to combat this sort of data breach and the money to implement those tools, could you improve data security at the IRS?

Answer. Yes. Additional data security tools, and funding for people, processes and technologies to implement those tools, would allow for significant improvements in data security at the IRS.

Congress can help by approving the President's FY 2016 Budget request for the IRS. The IRS budget includes $281 million (including 1,270 Full Time Equivalents (FTE)) specifically devoted to combating stolen identity refund fraud, cyber-security enhancements and related activities. This amount includes:

- $65 million to provide secure digital communications for taxpayers and provide leading-edge technologies to protect U.S. Treasury revenue through use of the IRS Return Review Program as well as advance IRS effectiveness in detecting, addressing, and preventing tax refund fraud;
- $42.6 million to enhance investigations of transnational organized crime;
- $40.7 million to address international and offshore compliance issues;
- $17.2 million to pursue employment tax and abusive tax schemes; and
- $8.2 million to improve taxpayer services through e-file authentication and mailing address data verification.

The budget also includes $188 million (including 157 FTE) for critical information technology infrastructure that will help ensure taxpayer data remains safe.

In FY 2017, the IRS will continue its commitment to taxpayers by building a new era of tax administration that will feature, among other priorities, stronger foundational capabilities and greater protection for the accounts of America's taxpayers. Additional funding will allow us to make these investments to strengthen cyber-defense and prevent identity theft and refund fraud by investing in technology and workforce skills that will allow for timely risk assessments, efficient analysis of vast volumes of data, and quicker reaction times to potential risks and incidents.

Data breaches and identity theft place a huge burden on their victims and present a challenge to businesses, organizations, and the IRS. The IRS is making progress against these crimes, but in the absence of sufficient resources and tools, these problems will continue and only compound over time.

Question. A number of my colleagues, including the Chairman and Ranking Member, Senator Nelson, and others, have introduced legislation addressing identity theft. The Individual Tax Reform Working Group, of which I am a co-chair, has been looking at identity theft and other tax administration issues. I hear from constituents who have fraudulent returns filed in their names, or whose family members are victimized by scammers, with very serious consequences and even heartbreaking consequences.

I hope that we will take up some of these proposals to prevent these issues in the near future.

Are there specific tools or proposals that would be especially helpful to you in efforts to prevent identity theft?

Answer. Congress can help us in the fight against refund fraud and identity theft by passing several important legislative proposals in the President's FY 2016 Budget proposal, including the following:

- **Acceleration of information return filing due dates.** Under current law, most information returns, including Forms 1099 and 1098, must be filed with the IRS by February 28 of the year following the year for which the information is being reported, while Form W–2 must be filed with the Social Security Administration (SSA) by the last day of February. The due date for filing information returns with the IRS or SSA is generally extended until March 31 if the returns are filed electronically. The Budget proposal would require these information returns to be filed earlier, which would assist the IRS in identifying fraudulent returns and reduce refund fraud, including refund fraud related to identity theft.
- **Correctible error authority.** The IRS has authority in limited circumstances to identify certain computation or other irregularities on returns and automatically adjust the return for a taxpayer, colloquially known as "math error authority." At various times, Congress has expanded this limited authority on a case-by-case basis to cover specific, newly enacted tax code amendments. The IRS would be able to significantly improve tax administration—including reducing improper payments and refund fraud as well as reducing costly audits—if Congress were to enact the Budget proposal to replace the existing specific grants of this authority with more general authority covering computation errors and incorrect use of IRS tables. Congress could also help in this regard by creating a new category of "correctible errors," allowing the IRS to fix errors in several specific situations, such as when a taxpayer's information does not match the data in certain government databases. To correct these errors today, IRS must open an audit, and we are limited in the number of audits we conduct by the resources available to engage with the taxpayer in the full audit process. Being able to correct certain mismatch errors would help with reducing some types of refund fraud.
- **Authority to regulate return preparers.** In the wake of court decisions striking down the IRS's authority to ensure unenrolled and unlicensed paid tax return preparers maintain minimum standards of competency, Congress should enact the Budget proposal to provide the agency with explicit authority to ensure all paid preparers maintain minimum standards. This legislation would help promote high quality services from tax return preparers and reduce refund fraud, improve voluntary compliance, foster taxpayer confidence in the fairness of the tax system, and protect taxpayers from preparer errors
- **Expanded access to Directory of New Hires.** Under current law, the IRS is permitted to access the Department of Health and Human Services' National Directory of New Hires only for purposes of enforcing the Earned Income Tax Credit and verifying employment reported on a tax return. The proposal would allow IRS access to the directory for tax administration purposes that include data matching, verification of taxpayer claims during return processing, preparation of substitute returns for non-compliant taxpayers, and identification of levy sources.

There are a number of other legislative proposals in the Administration's FY 2016 Budget request that would also assist the IRS in its efforts to combat identity theft, including: giving Treasury and the IRS authority to require or permit employers to mask a portion of an employee's SSN on W–2s, which would make it more difficult for identity thieves to steal SSNs; adding tax-related offenses to the list of crimes in the Aggravated Identity Theft Statute, which would subject criminals convicted of tax-related identity theft crimes to longer sentences than those that apply under current law; and adding a $5,000 civil penalty to the Internal Revenue Code for tax-related identity theft cases, to provide an additional enforcement tool that could be used in conjunction with criminal prosecutions.

It is important to note that these legislative proposals, while they would be very helpful, only would be partially effective in achieving their intended goals without adequate resources for the agency.

With limited resources and information, the IRS currently is only able to review fewer than 5% of the 100 million returns that request a refund. If, prior to issuing refunds, the IRS had access to third-party documents for matching earlier in the filing season (*e.g.,* W–2), the IRS would be able to identify fraudulent returns for

which there were no matching information returns. This would help reduce refund fraud, including refund fraud related to identity theft.

With additional resources, the IRS could implement the following improvements to protect revenue and taxpayers:

- Expand the pre-refund filters and improve systemic coverage of potential ID Theft returns;
- Increase the number of analysts manually reviewing filing patterns to identify new suspicious patterns and react to newly submitted leads; and
- Improve service to victims of identity theft by increasing the number of IRS employees who manually review returns, contact taxpayers when needed, and make account adjustments for taxpayers affected by ID Theft.

QUESTIONS SUBMITTED BY HON. MARK R. WARNER

Question. Commissioner Koskinen, based on your testimony, taxpayers used the Get Transcript application to successfully obtain over 20 million copies of their recently filed tax information. In previous statements, you have also mentioned that the "Where's my Refund?" application has been hugely successful. What does the IRS consider when balancing the availability of these services with protecting taxpayer's personally identifiable information?

Answer. In accordance with the National Institute Standards and Technology (NIST), the IRS has implemented a holistic, organization-wide Cyber-security risk management process with the principal goal of protecting the IRS organization and the ability to perform the IRS mission. The Cyber-security risk management process is treated as an essential management function of the organization balancing the assessment of management, operational, and technical controls to protect IRS systems. This approach includes applying NIST and Federal Information Security Management Act (FISMA) guidelines in identifying appropriate levels of identity proofing and authentication needed to protect IRS data and systems from identity and cyber-thieves.

We developed our on-line services to facilitate taxpayers' increasing demand for self-service and electronic service options by providing them with more web-based tools, to make their interactions with us simpler and easier. As part of that effort, we launched an updated version of the Where's My Refund (WMR) application for the 2003 filing season and the Get Transcript online application in January 2014. WMR enables taxpayers to check the status of their refund online or through their mobile device. Get Transcript allows taxpayers to view and print a copy of their prior-year tax information, also known as a transcript, in a matter of minutes. Prior to the introduction of this online tool, taxpayers had to wait five to seven days after placing an order by phone or by mail to receive a paper transcript by mail. Taxpayers use tax transcript information for a variety of financial activities, such as verifying income when applying for a mortgage or student loan.

During the 2015 filing season through May 22, 2015, taxpayers used WMR more than 217 million times. Without the WMR application, these contacts would have been driven primarily to our telephone application during a time when less than 40% of taxpayer calls were being answered.

Before the Get Transcript application was shut down for security reasons, taxpayers had used that application to successfully obtain approximately 23 million copies of their recently filed tax information during the 2015 filing season. If this application had not existed and these taxpayers had to call or write us to order a transcript, it would have stretched our limited resources even further. That point is important to note, given our limitations during the past filing season. We would have been much less efficient in providing taxpayer service, not to mention the additional burden placed on taxpayers.

The IRS considers many factors in making decisions around the appropriate level of identity proofing and authentication. Striking the right balance between a high level of confidence that the data and application are secure, and the ability of legitimate taxpayers to execute the authentication process and use the services, requires the IRS to make risk-based decisions. Today, striking the right balance between ease of access for legitimate taxpayers and protection of their data is an increasing challenge. As criminals obtain more personal information, authentication protocols need to become more sophisticated, moving beyond information that used to be

known only to individuals but now, in many cases, is readily available to criminal organizations from various sources.

The IRS continues to scrutinize and strengthen our authentication processes. In March 2015, we held a sit-down meeting with the leaders of the tax software and payroll industries and state tax administrators. We agreed to build on our cooperative efforts of the past and find new ways to leverage this public-private partnership to help battle identity theft.

We formed three working groups, one focusing on authentication, that continue to meet. They have agreed on short-term solutions to help taxpayers in the next tax season, and continue to work on longer-term efforts to protect the integrity of the nation's tax system. We identified numerous new data elements that can be shared at the time a tax return is filed to detect stolen identity refund fraud. Some issues we're focusing on include:

- Reviewing the transmission of the return, including the improper or repetitive use of Internet Protocol numbers, and the Internet address from which the return is originating.
- Reviewing computer device identification data tied to the return's origin.
- Reviewing the time it takes to complete a return, so computer mechanized fraud can be detected.
- Capturing meta-data in the computer transaction that will allow review for fraud.

This data will give us a stronger line of sight than ever before at the front end of the process and we believe this will help catch more bad returns immediately.

We must balance the strongest possible authentication processes with the ability of taxpayers to legitimately access their data and use IRS services online. The challenge will always be to keep up with, if not get ahead of, fraudsters in this area. The eventual approaches to authentication may include a combination of continued IT investments as well as modified business processes.

We continue to work with other federal agencies across government to identify best practices, leverage information and identify broader solutions. Ultimately, it is investment in our staffing and IT systems that will be critical to properly equipping the IRS to combat and prevent fraudulent and criminal activity.

Question. Commissioner Koskinen, last month, I co-sponsored the Social Security Identity Defense Act of 2015 with Senators Johnson and Ayotte. This bill would require the IRS to notify an individual if the agency has reason to believe the individual's Social Security Number has been fraudulently used. It also requires that the IRS notify law enforcement and that the Social Security Administration notify employers who submit fraudulently used Social Security Numbers. In addition to this legislation, I have written to you on several occasions to understand what the IRS is doing to notify victims of tax-related identity theft.

What steps is the IRS taking to notify victims of this recent attack, and what will you be doing in the future to protect their tax information?

Answer. Ensuring the security of our systems and the protection of taxpayers and their information are top priorities. Even with our constrained resources over the past few years, we continue to devote significant time and attention to these challenges. Ongoing data breaches involving other companies and organizations, through which criminals have been able to gather increasing amounts of personal data, make it even more challenging and difficult to protect taxpayers.

In May, the IRS determined unauthorized third parties already had sufficient information from a source outside the tax agency before accessing the Get Transcript application. This allowed them to clear a multi-step authentication process, including several personal verification questions that typically are only known by the taxpayer.

When the IRS first identified the problem in May, we determined that these third parties with taxpayer-specific sensitive data from non-IRS sources had cleared the Get Transcript verification process on about 114,000 total attempts. In addition, it appeared at that time that third parties made another 111,000 attempts that failed to pass the final verification step, meaning they were unable to access account information through the Get Transcript service.

Since then, as part of the IRS's continued efforts to protect taxpayer data, the IRS conducted a deeper analysis over a wider time period covering the 2015 filing season, analyzing more than 23 million uses of the Get Transcript system. The new review identified an estimated additional 220,000 attempts where individuals with taxpayer-specific sensitive data cleared the Get Transcript verification process. The review also identified an additional 170,000 suspected attempts that failed to clear the authentication processes.

The IRS mailed letters to all taxpayers identified in May and later we also mailed letters to the population identified in August (as part of our continued analysis). To the taxpayers whose tax information was successfully obtained by unauthorized third parties, we are offering credit monitoring, at our expense. We strongly encourage the recipients of these letters to take advantage of the credit monitoring. We are also giving them the opportunity to provide us with the authentication documentation necessary to get an Identity Protection Personal Identification Number (IP PIN). This will further safeguard their IRS accounts and help them avoid any problems filing returns in future years. The IRS is marking all of the impacted accounts will indicators that will help identify and prevent any fraudulent returns from being filed under those SSNs.

The Get Transcript application was shut down in May, and the IRS continues to work on strengthening the system. In the meantime, taxpayers have several other options to obtain transcripts.

The IRS takes the security of taxpayer data extremely seriously, and we are working aggressively to protect affected taxpayers and continue to strengthen our systems.

The matter remains under review by the Treasury Inspector General for Tax Administration as well as IRS Criminal Investigation.

Question. Commissioner Koskinen, the nation's economy and Americans' personal and financial information are increasingly under threat from cyber-attacks aimed at stealing personal data. In recent years, hundreds of millions of Americans have had their information compromised through high-profile breaches at Target, Neiman Marcus, Michaels, Home Depot, JPMorgan and Anthem.

I am working on a proposal to create a comprehensive, nationwide and uniform data breach law that is consistently applied and enforced across industries, and requires minimum data security standards and consumer notification for breaches of financial data and other sensitive information.

This recent theft at the IRS of over 100,000 taxpayer records by sophisticated attackers is yet another example of how stolen personal data can perpetuate an even larger fraud problem. What is the IRS doing to understand and react to the newest developments in cyber-security and data breach?

Answer. Cyber-security is a primary component of the IRS's information technology infrastructure. We use a proactive, layered set of cyber-defenses, and we assess risks in our management approach. The IRS's policy is to assume that a penetration can occur, and so we focus on prevention, constantly assessing our digital defenses, seeking to detect intrusions rapidly, quarantining infections, and taking prompt counter measures. The IRS works closely with partners in the Federal Government, such as: the Treasury Department's Government Security Operations Center (GSOC); the Department of Homeland Security's (DHS) Computer Emergency Readiness Team (US–CERT) as well as DHS's Government Forum of Incident Response and Security Team (GFIRST); and the Treasury Inspector General for Tax Administration (TIGTA).

While the IRS has a long history of successfully defending against attempts to steal taxpayer data, constant vigilance is needed, as the Get Transcript incident shows. Currently, the IRS takes a very aggressive approach to protecting taxpayer data by: restricting internet access; encryption of taxpayer data for any transmission externally; content filtering and strict firewall policies, and network security monitoring. In fact, the IRS has developed a Cyber-security Strategy that is focused on managing information security risk on a continuous basis; monitoring the security controls in IRS information systems and the environments in which those systems operate on an ongoing basis; and maintaining ongoing awareness of information security, vulnerabilities and threats to support organizational risk management decisions. The critical risk to continuing to implement this strategy is not the sophistication or frequency of cyber-attacks, but instead is the IRS's current budget situation which has resulted in the reduction of Cyber-security staff and the inability to

fill vacant positions. These skill sets and talents are under high demand across both the public and private sectors. The IRS's Cyber-security staff is currently 356 personnel, which is down from its high of 408 employees in FY 2012. The inability to hire and retain certified Cyber-security staff prevents the IRS from sustaining its vigilance against cyber-attack.

In addition to addressing the cyber-security issues of today, the IRS is working to anticipate the challenges of evolving technology used by taxpayers. The IRS is currently trying to move to a more robust interactive web-based means of interacting with taxpayers. The American people have grown accustomed to instant financial exchanges with lenders, brokers, and banks. The IRS believes that delivering top quality service to America's taxpayers requires catching up to those expectations in order to operate seamlessly but securely in a digital and global environment.

This evolution will increase cyber-security risks, requiring more resilience and protection of data. In response to the recent fraud incident referenced in your question, we are reviewing multiple authentication policies and capabilities with particular focus on updating our e-Authentication system for accessing a variety of online applications. The IRS is researching internal capabilities as well as those available from third parties through existing and planned contracts. These options include, but are not limited to:

- Internal IRS configuration updates to limit fraud and vulnerabilities to scripting attacks;
- Implementing the ability to add additional levels of assurance;
- Layering additional capabilities such as multi-factor authentication to complement assurance gained through taxpayer interactions; and
- Third-party configuration changes to improve and strengthen out-of-wallet questions for applications with the ability to use this type of authentication, such as online payment options.

We must balance the strongest possible authentication processes with the ability of taxpayers to legitimately access their data and use IRS services online. The challenge will always be to get ahead of our enemies in this area.

In addition to e-authentication improvements, the IRS also plans to enhance return filing by conducting the Processing Year W–2 Verification Code Pilot which will test the capability of a hash-based authentication code. The test will confirm the authenticity of Forms W–2 data on a pilot population of e-filed Forms 1040. The pilot is one of multiple IRS efforts to develop capabilities for authenticating taxpayers, and taxpayer data, at the point of filing to prevent identity theft and first party refund fraud.

And finally, Cyber-security and related initiatives submitted as part of the President's FY 2016 budget submission are specifically devoted to combating identity theft and refund fraud, as well as investing in critical information technology infrastructure. These initiatives will help enhance security in digital communications for taxpayers; provide leading-edge technologies to protect tax revenue through use of the IRS Return Review Program as well as advance IRS effectiveness in detecting, addressing, and preventing tax refund fraud; and improve taxpayer services with e-file authentication enhancements.

Question. Commissioner Koskinen, it is my understanding that third-party vendors have signed up with the IRS to access taxpayer transcripts via the Income Verification Express Service. What is the IRS doing to ensure that these third-party vendors that have signed up with the IRS to access taxpayer transcripts have appropriate safeguards in place and are not vulnerable to data breaches?

Answer. The IRS discloses return information to an Income Verification Express Services (IVES) participant pursuant to the taxpayer's authorization and request pursuant to Internal Revenue Code (IRC) section 6103(c). The taxpayer provides this authorization by completing and signing Form 4506–T, Request for Transcript of Tax Return. Form 4506–T includes this important statement to the taxpayer:

> Caution. If the tax transcript is being mailed to a third party, ensure that you have filled in lines 6 through 9 before signing. Sign and date the form once you have filled in these lines. Completing these steps helps to protect your privacy. Once the IRS discloses your tax transcript to the third party listed on line 5, the IRS has no control over what the third party does with the information. If you would like to limit the third party's authority to disclose your transcript in-

formation, you can specify this limitation in your written agreement with the third party.

Once the IRS discloses the information to the IVES participant pursuant to a valid Form 4605–T authorization, the IRS generally has no legal control over what the third party does with the information.

The IRS added a checkbox to Form 13803, IVES Applicant Agreement, listing additional limited use or non-disclosure restrictions. The checkbox states:

> By marking this box, you acknowledge that you have read Publication 4557, *Safeguarding Taxpayer Data,* and will abide by the guidelines of the publication. In addition, you agree to use the taxpayer information you receive only for the purpose(s) the taxpayer/requestor intended on the Form 4506–T. Failure to complete this box will result in the application being rejected and returned.

By checking the box, each IVES applicant acknowledges these non-disclosure restrictions as a condition of participating in the program. In addition, Publication 4557 addresses the responsibility of non-government service providers to secure information systems and security systems in addition to facilities and personal security required.

SUBMITTED BY HON. PAT ROBERTS, A U.S. SENATOR FROM KANSAS

The New York Times

MAY 28, 2015

I.R.S. DATA BREACH MAY BE SIGN OF MORE PERSONALIZED SCHEMES

By Patricia Cohen

The plot to steal information on 100,000 taxpayers from the Internal Revenue Service and hijack nearly $50 million in refunds not only reveals a previous security breach but hints at a wider fraud that may bedevil Americans in the future.

Some security and tax experts warned that this latest data theft might be a prelude to more targeted schemes aimed at duping taxpayers into handing millions of dollars over to criminals or to help thieves circumvent the agency's security filters next year and beyond.

"This breach is not just about what this single group is going to do with the information, but what happens when this information gets sold on the black market," said Peter Warren Singer, the author of "Cybersecurity and Cyberwar: What Everyone Needs to Know." "It's rare for the actual attackers to turn the information directly into money. They're stealing the data and selling it off to other people."

It is almost impossible to find a business or government agency that has not had some kind of security breach, he noted. Millions of customers at companies like Target and the private insurer Anthem have had data compromised. And this year, TurboTax temporarily halted electronic filing of state income tax returns after seeing an uptick in attempts to use stolen information to file fraudulent returns and wrongly claim tax refunds.

With the I.R.S., it was not the agency's own system that was hacked. Criminals had already obtained individuals' Social Security Numbers, addresses and birth dates and then used the information to trick the network and gain access to taxpayers' returns and filings through an application on the I.R.S. website.

"There was no identity theft within the I.R.S.'s actual system," said Aaron Blau, a tax expert in Tempe, AZ. "These people already had all of this data. They could have used this information to call your bank, your doctor, your insurance carrier, and they would have gotten through 100 percent of the time. In this case they chose to use the I.R.S."

Many Americans are being attacked more directly, Mr. Blau said. One popular scheme is to cold-call taxpayers and threaten them with prosecution if they do not immediately pay money supposedly owed to the I.R.S. by directing them to purchase a prepaid debit card and then transfer the money. Now, with more detailed information from returns, criminals could better target potential victims, and bolster their credibility with information stolen from taxpayer filings, Mr. Blau said.

Reusable prepaid cards have become a magnet for fraud, according to law enforcement officials, with criminals often posing as bill collectors, government agents and others.

Without more information about the individuals who were targeted, it is hard to know the endgame, said Marc Goodman, the author of "Future Crimes." Mr. Goodman noted that previous security breaches had sometimes been used to embarrass politicians, celebrities or corporate figures, and tax returns would provide a rich source of personal information.

Although some critics have been quick to condemn the I.R.S., several tax experts said using this episode to vilify the agency was unfair.

"The I.R.S. takes data, privacy and data security extremely seriously," said Edward Kleinbard, a professor of law at the University of Southern California and former staff director of the Joint Tax Committee of Congress. "They do their best, but the resources arrayed against it have become increasingly well-funded and sophisticated, and the problems will only compound over time."

William Gale, co-director of the tax policy center at the Brookings Institution, agreed that the issue extended beyond a single agency. "I don't think this is an I.R.S. problem per se. It is facing the same problems that all the major data providers have."

The I.R.S. has repeatedly said that protecting taxpayer information and combating fraud were priorities. Half of the attempted information thefts were rebuffed through a system of filters that are used to detect fraud, the agency said.

Still, there is little debate that its efforts have been hampered by budget cuts. Just two months ago, an agency overseer issued what now seems to be a prescient warning.

"Resources have not been sufficient for the I.R.S. to work identity theft cases dealing with refund fraud, which continues to be a concern," J. Russell George, the Treasury Inspector General for Tax Administration, testified before a Senate subcommittee.

The agency's budget has been cut by 17 percent over the last four years after taking inflation into account, and its work force, now at roughly 83,000, has been reduced by 12,000. This year, John A. Koskinen, the I.R.S. commissioner, warned that impending budget cuts would have devastating effects, including the delay of new protections against identity theft and refund fraud.

Chuck Marr, director of federal tax policy at the Center on Budget and Policy Priorities in Washington, said that the agency has been starved for funds: "The Congress has been targeting the I.R.S. for years."

Nina E. Olson, who leads the Taxpayer Advocate Service, an independent office at the I.R.S., has criticized the agency for its handling of identity theft cases.

In her annual report, she noted that victims often must "navigate a labyrinth of I.R.S. operations and recount their experience time and again to different employees. Even when cases remain in one I.R.S. function, they may be transferred from one assistor to another with significant periods of non-activity." On average, the agency took nearly six months to resolve cases.

She added that cases were also frequently closed prematurely, "before all related issues have been fully addressed."

Her office recommended that a single officer be assigned to handle each case.

In an email, she spoke to a broader issue: "While granting taxpayers enhanced access to their tax information remains a laudable goal, the overriding priority must be to protect taxpayers' confidential tax information from exposure."

As for this most recent data theft, the I.R.S. urged taxpayers not to contact the agency, saying it would only delay the already overburdened staff. Anyone whose information was stolen will be contacted, the agency said.

The best advice at this stage, Mr. Blau, the tax expert, said, is, "Hurry up and wait."

PREPARED STATEMENT OF HON. RON WYDEN,
A U.S. SENATOR FROM OREGON

Three months ago, the Finance Committee met in a hearing on the latest ID theft and other scams plaguing taxpayers, and I said that wave of attacks sure looks to me like organized crime. Today, we meet after 104,000 tax returns have been hoovered up by what appears to be a sophisticated organized crime syndicate.

This problem continues to spiral, with hackers targeting Federal agencies, State governments including Oregon's, and private companies alike to steal money and data. One recent report from the Department of Homeland Security said federal agencies' computer systems come under attack hundreds of times a day, tens of thousands of times a year.

The investigation of the stolen tax returns is ongoing as of this morning. But once again, it seems the thieves are one step ahead of the authorities. They gained access to enormous amounts of personal data, which is up for purchase at extraordinary cost in the Internet's shadowy corners. These rip-off artists used that data to slip past the security filters at the IRS and steal taxpayers' most sensitive financial information.

So in my view, it's fair to say that once again, this conduct fits the definition of organized crime.

The thieves who steal taxpayer information could wipe out people's life savings and leave them in financial ruin. They could falsify tax returns next year or further down the road. They could take out huge, fraudulent home or student loans. And on a bigger scale, the money stolen in this cyber-crime wave could be funneled into more criminal activity. It could wind up in war zones. There's a possibility that it could fund acts of terrorism without being traced.

Just like when the White House and the Department of Defense were targeted in the past, this was an attack on Americans' security. I will be very direct about what's needed here. To protect taxpayers from this onslaught of cyber-crime, the IRS needs a 21st-century IT system.

This is not just a question of resources, and certainly it is not a lack of commitment from the IRS staff. It's also a question of expertise. The era of punch cards and paper forms ended long ago. Federal agencies like the IRS need to tap into the expertise of our leading web firms—the pros who serve not millions or tens of millions, but hundreds of millions of users.

That expertise will allow the IRS to avoid the pitfalls of the past and to implement a 21st-century IT system that protects taxpayers' privacy, catches hackers and cheats, and funds the government as efficiently as possible. When that system is in place, Congress must step up and appropriate the funds necessary to manage it effectively.

Legislators would not call for the DOD or White House security budgets to be slashed after cyber-attacks, but the IRS's security funding has been shrinking for years. No company would try to defend against modern cyber-criminals with technology that's 20 or 30 years old, but that's what the IRS is stuck using in the absence of the expertise and resources to serve the American taxpayer.

Congress could also make sure the IRS has the information it needs to mount the strongest possible fight against fraudsters. If the IRS had access to the data on W–2 and 1099 forms from the very beginning of tax season, it would be much easier to catch fraudulent returns early and save taxpayers the nightmare of a stolen refund. Senator Hatch and I developed a bipartisan proposal to add an extra level of security by expanding the program that distributes unique passwords for individual taxpayers to use when they file.

And when taxpayers do become victims of fraud, they should get more help undoing the damage quickly and restoring their credit.

It should be clear to everybody that beefing up cyber-security at the IRS must be a top priority and draw on the tech expertise that exists in Oregon and in states across the country. So it's my hope that our hearing today will set aside politics and focus on fresh ideas of how to best protect taxpayers.